DOCUMENT RESUME

ED 168 463 IR 006 883

TITLE	A Computer Network Protocol for Library and Information Science Applications. NCLIS/NBS Task Force on Computer Network Protocol.
INSTITUTION	National Bureau of Standards (DOC), Washington, D.C.; National Commission on Libraries and Information Science, Washington, D. C.
PUB DATE	Dec 77
NOTE	101p.
AVAILABLE FROM	Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402 (Stock No. 052-003-00601-4, $2.75)
EDRS PRICE	MF01/PC05 Plus Postage.
DESCRIPTORS	Computer Programs; Computers; Data Bases; Information Science; *Information Systems; Library Automation; *Library Networks; Library Technical Processes; *On Line Systems; *Standards

ABSTRACT

This document describes a proposed computer to computer protocol for electronic communication of digital information over a nationwide library bibliographic network. The protocol allows application tasks at one site on the network to converse with application tasks at any other site, regardless of differences in computer architecture or operating systems. The protocol relies on other standard protocols for supplying a reliable communications network. The physical network environment to implement this protocol can be structured in a variety of ways and might utilize facilities supplied by common carriers, value added networks, or a combination of both. The Task Force suggests that further investigation remains to be done in the areas of implementation details and program impact. (Author/JVP)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED168463

U S DEPARTMENT OF HEALTH, EDUCATION & WELFARE
NATIONAL INSTITUTE OF EDUCATION

THIS DOCUMENT HAS BEEN REPRODUCED EXACTLY AS RECEIVED FROM THE PERSON OR ORGANIZATION ORIGINATING IT. POINTS OF VIEW OR OPINIONS STATED DO NOT NECESSARILY REPRESENT OFFICIAL NATIONAL INSTITUTE OF EDUCATION POSITION OR POLICY

A COMPUTER NETWORK PROTOCOL FOR LIBRARY AND INFORMATION SCIENCE APPLICATIONS

NCLIS/NBS Task Force

On Computer Network Protocol

The views, opinions, and recommendations expressed in this report are those of the National Commission on Libraries and Information Science/National Bureau of Standards Task Force on Computer Network Protocol and do not necessarily reflect official position or policy of either the National Commission on Libraries and Information Science or the National Bureau of Standards.

National Commission on Libraries and Information Science

1717 K Street, N.W. Suite 601

Washington, D.C. 20036

1977 December

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402

Stock No. 052-003-00601-4

LC00883

Library of Congress Cataloging in Publication Data

NCLIS/NBS Task Force on Computer Network Protocol.
A computer network protocol for library and information science applications.

Bibliography: p.
1. Library information networks--Standards--United States. 2. Libraries--Communication systems--Standards--United States. 3. Library science--Data processing--Standards--United States. I. Title.

Z680.3.N18 1977 021.6'5'0973 78-9898

PREFACE

Several events preceded the establishment of the NCLIS/NBS Task Force on Computer Network Protocol. These events provide informative background data concerning the responsibilities and scope of the Task Force.

The Telecommunications Committee (TC) of the American Library Association's Information Science and Automation Division (ISAD) spent one year, in its biannual meetings, developing a framework for a computer-to-computer communications protocol. While a report of ISAD's work eventually was published as a Technical Communication in the Journal of Library Automation, development was hampered by the committee's infrequent meetings and changing membership.

In addressing an ISAD meeting about the work of the National Commission on Libraries and Information Science (NCLIS), Joseph Becker urged ISAD to consider participating in the development of a national network postulated by NCLIS. Henriette Avram, then President of ISAD, took the matter before the ISAD Board of Directors. Consequently, Alphonse Trezza, Executive Director of NCLIS, made a presentation to the ISAD Board at the 1976 ALA Midwinter Meeting.

As a result of Mr. Trezza's presentation, the Board agreed that the efforts by the ISAD TC to define a computer-to-computer protocol would be an appropriate activity to continue under NCLIS sponsorship.

A series of discussions followed among Henriette Avram, Alphonse Trezza, NCLIS staff, and Phil Long, Chairman of the Telecommunications Committee. During the discussions, the project was defined, participants were identified, and an appropriate work statement was developed. While it was clear that to work effectively the proposed Task Force membership should be kept to a minimum, it was also clear that representation should encompass a broad constituency of interested and affected communities. Also, since the initial assumption was that a proposed standard would result from the project, it seemed imperative to involve the National Bureau of Standards in the project.

The structure of the Task Force was set to include a team of nine members and one chairman. In addition, invitations were extended to interested members of the for-profit community to serve as technical consultants. The project was conducted under the auspices of the Institute for Computer Sciences and Technology (ICST) of the National Bureau of Standards with funding provided by NCLIS.

The actual membership of the Task Force included knowledgeable individuals in the library community some of whom also represented ISAD library and information-related associations, the Tele-

communications Committee, the National Federation of Abstracting and Indexing Services (NFAIS), and ARPANET. Technical consultants included representatives from the Information Industry Association (IIA), Tymnet, Telenet, and the publishing community. A member of NCLIS also was appointed to the Task Force. All meetings were announced in the Federal Register. The Task Force was chaired by Ruth L. Tighe of NCLIS; John L. Little of the National Bureau of Standards acted as Task Force Coordinator. The original Task Force included: Team Members: James K. Barrentine, Hanan S. Bell, Howard C. Berkowitz, John D. Day, Nick A. Farmer, James G. Hale, Jr., Philip L. Long, Clarice I. MacDonald, and William D. Mathews. Technical Consultants: Arthur J. Caisse, Jack Speer, Barbara R. Sternick, Barry D. Wessler, and David Wolverton. Other Participants: Henriette Avram, George E. Clark, Jr., Madeline Henderson, Stephen R. Kimbleton, Albrecht J. Neumann, and Thomas N. Pyke, Jr.

While composition of the Task Force shifted in the process of the project, participation continued to be high and contributed significantly to the quality of the final product of the Task Force. Appendix A reflects the membership of the Task Force as it was finally constituted.

NCLIS wishes to express its grateful appreciation to the members of the Task Force for their diligent efforts; to their sponsoring organizations for their generous donations of staff time; to the National Bureau of Standards for its many efficient services; to Jim Barrentine for providing text-editing and processing of the final report through its several iterations; and to Peggy Zimbeck without whose continuing editorial efforts, production of the report would have been immeasurably more difficult.

TABLE OF CONTENTS

		Page
PREFACE		i
TABLE OF CONTENTS		iii
LIST OF TABLES		v
EXECUTIVE SUMMARY		vii
I.	INTRODUCTION	1
II.	EXISTING ENVIRONMENT FOR THE NETWORK	2
	A. Participating Organizations - Suppliers	2
	B. Participating Organizations - Users	3
	C. Functional Areas and Applications for Automation	3
	D. Summary	5
III.	TASK FORCE RESPONSIBILITY	7
	A. Communications Methodology	7
	B. Application Level Protocol	9
	C. Protocol Data Requirements	10
	D. Summary	11
IV.	GENERALIZED MODEL	12
	A. The Network Protocol Requirements	12
	B. Network Model Assumptions	13
	C. Application Transactions	14
	D. Transaction Message Flows	16
	E. Registry	16
V.	PROTOCOL	19
	A. Terminology	19
	B. Protocol Assumptions	19
	C. Message Classes	20
	D. Message Format	21
	E. Required Header Fields	22
	F. Optional Header Fields	27
	G. Control Messages	34
	H. Data Type Messages	46

Page

VI. SUMMARY AND RECOMMENDATIONS. 47

APPENDIX A. COMPOSITION OF THE TASK FORCE. 49

APPENDIX B: AN EVALUATION OF LOWER LEVEL PROTOCOLS. 52

APPENDIX C: GLOSSARY 60

APPENDIX D: SUMMARY OF HEADER FIELDS PRESENT IN MESSAGES. 70

APPENDIX E: SAMPLE SESSION - INTERLIBRARY LOAN . . . 71

APPENDIX F: STATE DIAGRAMS 79

APPENDIX G: BIBLIOGRAPHY 88

LIST OF TABLES AND FIGURES

		Page
Figure III.1:	PROTOCOL LEVELS.	8
Figure III.2:	MESSAGE FLOW BETWEEN LEVELS.	9
Figure IV.1:	NETWORK STRUCTURE.	12
Figure IV.2:	NETWORK STRUCTURE SHOWING APPLICATION PROCESSES.	13
Table IV.3:	FUNCTIONS AND TRANSACTIONS	17
Table IV.4:	TRANSACTION FLOW	18
Figure V.1:	DETAILED MESSAGE STRUCTURE	24
Table V.2:	FLAG BITS AND MEANINGS	25
Figure V.3:	USE OF REFERENCE NUMBERS	26
Table E.1:	OVERVIEW OF THE SAMPLE SESSION	74

EXECUTIVE SUMMARY

This document describes a proposed computer-to-computer protocol for electronic communication of digital information over a nationwide library bibliographic network. The protocol allows application tasks at one site on the network to converse with application tasks at any other site, regardless of differences in computer architecture or operating systems.

The protocol relies on other standard protocols for supplying a reliable communications subnetwork. The physical network environment to implement this protocol can be structured in a variety of ways and might utilize facilities supplied by common carriers, value added networks, or a combination thereof.

The formulation of this protocol represents the clearing away of a major, time-consuming, technical roadblock which impeded the establishment of a coherent nationwide library bibliographic network. While it is felt that this protocol will ultimately have an important impact on the configuration of library and information services, this impact has not been studied in detail. Moreover, additional related technical areas still require attention.

Specifically, while this recommendation is as complete as many other protocols which have become national standards, several requirements must be fulfilled before it can actually be proposed to a standards-making body. The Task Force recommends that this issue be further investigated.

Moreover, a great many implementation details -- such as error recovery, exceptions, relationships between the protocol and the host operating systems-- will only be understood in their fullest as the protocol is implemented. The Task Force suggests that a pilot implementation of the protocol be undertaken.

Finally, in order to effectively use the protocol, a number of codes must be assigned and made known to the users. The Task Force recommends that this "registry" function be established and that further orderly development of the protocol be insured by establishing appropriate agents for carrying out this work.

I. INTRODUCTION

Over the past several decades, libraries have relied increasingly on cooperative ventures in resource sharing to improve service to their patrons. This cooperation often takes the form of interlibrary loans and union catalogs. With the increasing trend towards automation of many library functions, libraries are looking for ways to interconnect their often dissimilar computers and further augment cooperation. Libraries have begun to take advantage of computerized information services to provide new access routes to information for their patrons. With these additional opportunities for information and resource sharing now available, attention has focused on standardizing communications among organizations wishing to interconnect their computers.

Several groups and committees have worked in this critical area of standardization. The Telecommunications Committee of the Information Science and Automation Division (ISAD/TC) of the American Library Association spent several months developing a framework for a computer-to-computer communications protocol. Their effort culminated in a technical communication published in the 1976 June issue of the Journal of Library Automation.

The ISAD/TC Committee concluded that a more concentrated effort was needed if substantial progress was to be made in defining a generalized, application level, computer-to-computer protocol. In response to the ISAD's initiatives, the National Commission on Libraries and Information Science (NCLIS), in cooperation with the National Bureau of Standards (NBS), formed a Task Force in 1976 September. The Task Force, comprising representatives from the library and information science community, was to develop a computer-to-computer protocol for the proposed Bibliographic Component of the National Library and Information Science Network (subsequently called "the Network"). Members of the Task Force met several times over a 12-month period in both public plenary sessions and small ad-hoc working subgroups. This report represents the results of that one-year effort.

II. EXISTING ENVIRONMENT FOR THE NETWORK

The following presentation of the existing environment in which the Network will grow can provide the reader with a better basis for understanding the proposed protocol. First, the Network environment is described in terms of the participating organizations, some of which are information suppliers and others which are information users. Second, the Network environment is described in terms of the functions or application areas which are traditionally amenable to automation within the library.

A. Participating Organizations - Suppliers

Government agencies, both national and international, play a substantial role as suppliers of bibliographic information to libraries. The Library of Congress, National Agricultural Library, National Library of Medicine and other U.S. Federal agencies and libraries are important contributors of authoritative cataloging and other data. National libraries in other countries such as The Bibliotheque Nationale also play an important role as generators of bibliographic information. Clearly, international standards are an important consideration in the development of the Network.

Bibliographic service centers and regional library networks are emerging as a strong influence in information transfer among libraries. Service centers such as BALLOTS, OCLC, Inc. and the Washington Library Network (WLN) provide on-line access to cataloging data bases. Regional networks such as AMIGOS, NELINET, PALINET, and SOLINET are defining a role for themselves in the efficient distribution and delivery of services by means of telecommunication links to libraries across the country. Many of these service centers and regional networks are membership-operated organizations, controlled by the libraries which receive the services.

Professional societies, particularly in the sciences, contribute significantly to machine-readable abstracting and indexing data. The publications and services of the Chemical Abstracts Service and the Engineering Index are good examples of these contributions. In their printed form, these indexes are a main source of access and control for the vast resource of journal and report literature in the field. In machine-readable form, these indexes are available for on-line use through various service centers.

A diversity of corporations in the private sector is information-related and thus relevant to the Network as suppliers of library services. Baker and Taylor, Blackwell, Brodart, Faxon, and other book jobbers and periodical subscription service agencies naturally are interested in refining the process of materials ordering and invoicing in libraries. This refinement of

operations also directly involves hundreds of publishers across the country such as Bowker, Wilson and Xerox who produce bibliographic data as end products. Lockheed and the System Development Corporation are notable for providing on-line access to abstracting and indexing data through their large computer centers. Telenet, Tymnet and other value-added carriers provide reliable user-to-computer and computer-to-computer interconnections; together with the common carriers, these value-added carriers likely will provide transmission services for any library network. CLSI, Gaylord, Plessy, 3M, and others are active software houses that produce turnkey systems on small computers for direct use in library applications. Finally, hardware manufacturers of computers, communications equipment and terminals supply the physical components so vital to the operational success of a network. Recent developments by hardware manufacturers in character recognition hardware, typesetting, key entry, point-of-sale and banking equipment are relevant to the development of the Network protocol.

B. Participating Organizations - Users

As users of information services, Federal libraries and Federal agencies again play an important part in the Network environment. For example, the Library of Congress supports the Congressional Research Service, and the National Library of Medicine provides various information services for its users. College and university libraries, generally located in more populated areas accessible to telecommunication lines, contain a substantial portion of the nation's literary wealth and provide patron service for the educational community. Public libraries numbering in the thousands are frequently located in isolated rural areas. Libraries located in rural areas, whether educational or public libraries, pose special problems for highly distributed, low cost telecommunications. Special libraries and information centers serving corporations also pose special problems in that they usually have small collections and rely heavily on interlibrary loan.

In all of these examples, the major goal of these organizations is to provide information services to individuals. The Network will ultimately be measured by how well it improves information services to the individual citizen.

C. Functional Areas and Applications for Automation

Libraries are involved primarily in the business of information collection, organization, dissemination, and use. These tasks translate respectively into the functional areas of acquisitions, cataloging, circulation, and reference, all of which have been facilitated by computer systems.

Acquisitions of library resources occur when collection building policies are translated into decisions to acquire material in a particular subject area. Widely defined, acquisitions systems control and report on the flow of material from the time an item is ordered until it is on the shelf and ready for patron use. Specifically, acquisitions systems guide and oversee the ordering, receipt claiming, cancellation, and cataloging workflow in a library. Monographs, serials, journals, and government documents are examples of types of publications that must be handled by acquisitions systems. Media forms such as phonodisc, videotape, and microfiche also must be accommodated by the acquisitions process as readily as materials in the more traditional printed form are accommodated.

Acquisitions of serials pose special problems for libraries. Although serials processing parallels monographic processing, the open-ended, repetitive and unpredictable routine of serials publishing indicates that special systems should be developed for serials processing. Serials processing therefore is often handled by separate departments in the library and by separate software systems. Serials systems frequently must provide for check-in, claiming and binding control within their departments.

In addition to controlling the flow of material, acquisitions systems also account for the flow of money through invoice processing and fund accounting. It is in this area that acquisitions systems tend to be highly ideosyncratic, i.e., highly specialized to the needs of an institution. Design decisions in this area are usually dictated by the larger institution or administrative division to which the library belongs. It would be extremely beneficial to libraries if book jobbers and publishers could be "connected" to libraries in such a way that orders, invoices, claims, and cancellations could be transferred in a standard machine-readable format. As an output control, acquisitions systems provide detailed data on the status of items as they move through the technical processing areas of a library, maintain control over hundreds of funds and accounts, and supply much-needed management information and statistics to library administrators.

The cataloging process includes the intellectual organization, description and classification of material. Major emphasis in cataloging focuses on the integrity and accuracy of the information being placed in the catalog. For this purpose, ready access to an authoritative data base of cataloging records is of considerable importance to libraries. Equally important is standardization and consistency of access points to the data base. Automated updating and selection of information from subject, name, and other authority files are now possible and can directly support access points to the cataloging data base. The direct product of cataloging systems is the catalog itself, on card, book, microform, or machine-readable media. By-products of the cataloging process include accessions lists, holdings lists, and union catalogs.

Circulation is the process of lending known items to known users for specific lengths of time. Circulation systems function as an inventory control over items in the library, providing location data as to whether a specific item is available in the library or is on loan to a patron. Interlibrary loan is a special case of circulation and in itself places heavy communication and record keeping demands on a library. Management of reserve book collections in academic libraries also is viewed as a special case of circulation where a collection is brought together rapidly at the beginning of an academic term. Direct outputs of circulation systems are overdue notices, lists of items out on loan, and statistical profiles of library use. Invariably library circulation systems manage lists of patron names and addresses. Some libraries have begun to use circulation information as feedback to the acquisitions process or as guidance in collection weeding.

From the library user's point of view, the library catalog serves as a primary reference service. Thus, direct on-line access by the patron to library catalogs would be extremely beneficial. Presently this capability seems to be economically out of reach. Reference use of other on-line search and retrieval services, particularly abstracting and indexing data, is an active reality in some libraries but in each case access is not provided over dedicated networks and is not integrated with other uses of automated systems within the library. Expanded reference services should permit user access to services of a broader text management and editorial nature where the user could create, arrange, sort, edit, and typeset bibliographic and other textual material provided by libraries. Reference use of census data is a "gray" area of information use which falls between text handling and computation. The printed form of the census often is found in a library but a user cannot access and manipulate the census data in machine-readable form. As libraries broaden their scope to include more diverse media, text handling and computational laboratories will become an increasingly common library phenomenon.

D. Summary

The Network cannot and should not be expected to supply systems for all the functions described above. Indeed, it seems likely that acquisitions and circulation control may be handled locally by turnkey systems. However, even the turnkey systems could benefit from deriving and transmitting information over the Network.

The cataloging and reference services, on the other hand, present strong arguments for widespread data sharing. Maintenance of authoritative files requires much work and creates sizeable file management demands. It is likely that the authority systems which access cataloging files will be located at large bibliographic processing centers for some time to come.

Most existing automated systems cannot be used directly in a network environment without improvement or alteration since library automation efforts on the whole have been isolated efforts. Since no national network yet exists, library systems have not been developed to accommodate the environment such a network would provide. However, it is expected that the Network will provide an information transfer vehicle which will inevitably unify, integrate, and reorient these otherwise diverse and disparate applications and organizations.

III. TASK FORCE RESPONSIBILITY

The preceding section addressed the environment in which the Network is expected to operate and grow. This section defines the characteristics of the Network, as perceived by the Task Force, and identifies which of the many tasks required to implement the Network will be addressed by the Task Force.

The library community comprises three major groups: the libraries themselves, individuals (or organizations) that use the services provided by the libraries, and organizations that in turn provide services to the libraries. In a global sense, the Network can be envisioned as some complex, highly connected, interactive collection of terminals and computers, with the nodes of the Network distributed among the three groups. While it is possible that the Network may evolve into that form, the Task Force envisions the Network in its initial form to be much simpler.

Initially, the Network probably will consist of the interconnection of the computers operated by: 1) bibliographic service centers such as BALLOTS, OCLC, and WLN; 2) the regional networks such as NELINET and SOLINET; 3) large libraries such as the Library of Congress and the New York Public Library; 4) members of the private sector. The Task Force feels it is through these organizations that the Network has the best chance of becoming a reality.

A. Communications Methodology

The goal of the Network is to facilitate resource sharing and to permit data transfer from one computing facility to another. (Computing facilities are usually geographically dispersed and remote from one another.) In order for this data transfer to take place in an orderly and efficient manner, several software and hardware components must interact in a complex fashion. This interaction is illustrated by the layered process diagrammed in Figure III.1.

In Figure III.1, solid lines denote real communication paths and dashed lines denote virtual communication paths. To effect communication across a virtual path, one must follow a real communication path up and/or down the various levels.

Since communication across a virtual path cannot be done directly, a methodology to accomplish the exchange using the physical communication paths must be developed. This methodology is called a protocol. Protocols are necessary to describe and define the mechanism of inter-level movement. For a given level, the protocol defines the data structure and procedures that are required for that level to communicate with its counterpart on the other side of the diagram.

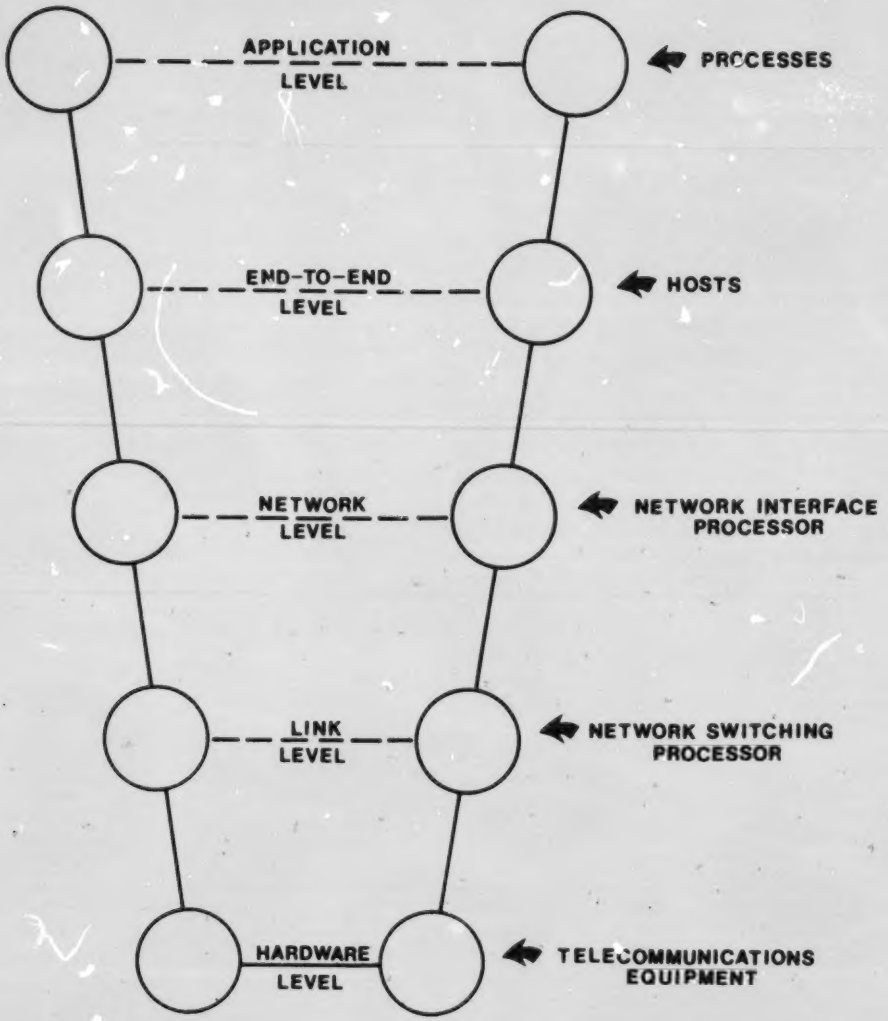


Figure III.1: PROTOCOL LEVELS

Some protocol implementations divide the data being passed between levels into control fields and information fields. The control fields contain data necessary for the protocol to function properly. The information fields contain data that are passed through the levels without inspection. As a message descends from level to level, the control and information fields of the previous level may become the information fields of the current level. The current level may append control fields to these information fields and send the message on to the next lower level. As a message ascends from level to level, the current level's control field is stripped off at that level before passing the remaining data upward. Note that this is a logical view and may or may not describe the physical methodology. Figure III.2 diagrams this message flow.

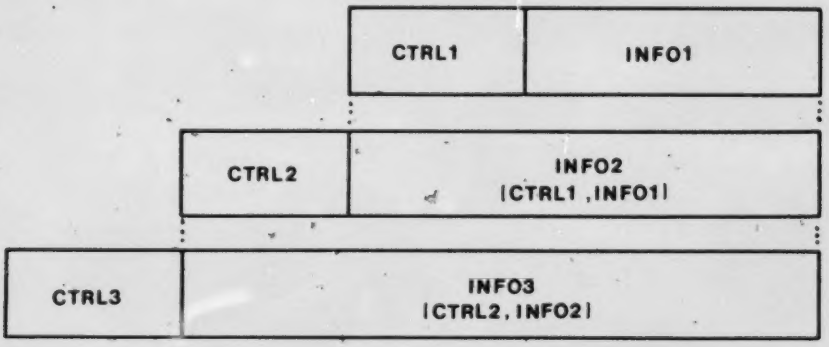


Figure III.2: MESSAGE FLOW BETWEEN LEVELS

B. Application Level Protocol

The Task Force is concerned with the protocol at the application level. That is, the Task Force has defined the standardized communications procedures that an application program (or more precisely the range of application programs that may exist in a library environment) at one host computer will use to address another application program operating on a different host computer. The fact that the other levels are present and necessary with all their attendant hardware and software is of no concern at the application level. The Task Force has assumed that the protocol at these other levels (hardware, link, network and end-to-end) are host and/or network controlled and combine to accomplish error-free transmission.

While the scope of the work of the Task Force has been limited to the definition of this highest level (application) protocol, the Task Force recognizes the importance of using standards at all levels.

The Network will consist of connections between host computers; it is not intended to support terminals directly. The main functions of the hosts will not be program development, general computations, generalized data base management services, dispersed multi-processing or any of the other activities typically associated with existing computer networks. Because of the limited scope of activities carried out by the Network, many of the problems faced by existing networks (e.g., the specification of a standard terminal, standard log-on protocol, network operating system and data base organization) have not been addressed by the Task Force. These areas will be the responsibility of the individual hosts of the Network (e.g., the decision as to which terminal to use) or they will be made transparent to the Network by the application software in the individual hosts (e.g., the characteristics of the data base management system being used).

C. Protocol Data Requirements

The messages passed between operational applications in the Network host computers will consist of two parts: a header and actual application data. The Task Force has addressed only the header portion of the message, but also notes the need for developing standards for the data portion of the message since the characteristics of these data may have a significant impact on the operation of the underlying communications network. Furthermore, the Task Force has proceeded on two assumptions: 1) the underlying communication network will be able to efficiently transfer the type of data used by application programs in a library environment; 2) the data communications link protocol will be a bit-oriented protocol and thus will not impose any restrictions on the types of data transmitted between the nodes of the network. Among data types currently envisioned are:

character data: The majority of data transmitted will be character data. A character code that might be used is ASCII 1977, or extensions to ASCII such as that used in the MARC code or as specified by ISO standards.

numeric data: Some numeric data, such as accounting or billing data, might be transmitted in a packed decimal format; other numeric data might be transmitted in binary format.

binary data: In addition to numeric data, the Network must be able to handle larger volumes of data in binary form such as that produced by a facsimile device.

In addition to the functional specifications listed above, there are several operational requirements that must be accepted by the organizations which constitute the nodes of the Network. These operational requirements include:

availability: The Network's hours of operation must be defined. Also, the problem of what actions must be taken when all or part of the Network is not operational must be addressed.

reliability: Metrics for acceptable error rates at all levels in the Network must be defined and responsibility for the detection/correction of error conditions must be assigned.

activity: Some rough measure of the expected Network activity should be developed. This measure should include the number of transactions that a node might be expected to receive, the rate at which transactions might arrive, and the average size of a transaction.

responsiveness: The speed at which the nodes must be able to respond to requests for service, in seconds, minutes, hours or days, should be specified.

While it is not the responsibility of the Task Force to define in any further detail these operational requirements, the Task Force acknowledges their importance.

D. Summary

In summary, the Task Force has addressed in detail only the application level protocol and has not defined the actual information that must be transmitted between Network hosts to execute a particular application. The Task Force has defined only the header information that must be transmitted between the application programs running at the host computers that constitute the Network. This header information is general enough to support a wide variety of applications typically found in library and information service environments.

IV. GENERALIZED MODEL

The Task Force used the generalized model described in this section to develop the protocol discussed in subsequent sections of this document. The model describes how communications between nodes will be established and controlled.

A. The Network Protocol Requirements

The Bibliographic Component of the National Library and Information Services Network consists of an interconnection of computerized services to libraries. The entities that will be connected by the Network include the computers at several bibliographic service centers, various types of authority centers, and vendors of library products and services. The Network will support various kinds of transactions occurring between the computerized entities connected to the Network and will provide a means of passing strings of data among the entities. One possible Network conceptualization has each of the entities connected to a communications subnetwork such as is depicted in Figure IV.1.

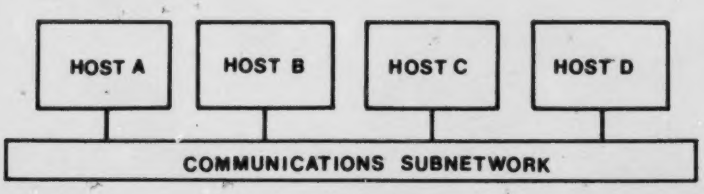


Figure IV.1: NETWORK STRUCTURE

This communications subnetwork will permit the transfer of information from any entity to any other entity and act as a fully interconnected net. No assumptions have been made about the actual physical interconnections. If entities are not directly connected to one another, the applications program need not to be aware of actual interconnections since these would take place at a lower level in the communications hierarchy.

Figure IV.2 depicts the four hosts connected to the communications subnetwork. These hosts provide library-oriented processes, usually called "applications": 'CAT' indicates a cataloging application; 'ACQ' indicates an acquisitions application; 'SER' indicates a serials control application; 'REF' indicates a reference application; and 'ILL' indicates an interlibrary loan application.

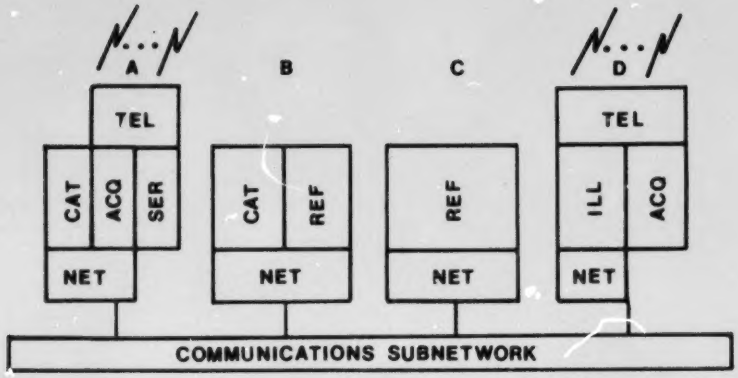


Figure IV.2: NETWORK STRUCTURE SHOWING APPLICATION PROCESSES

The following points should be noted on Figure IV.2:

1. The Network includes certain facilities associated with each host (designated 'NET') and all the interconnections between such 'NET' facilities.

2. The Network allows applications on one host to communicate with applications on another host. For example, the 'CAT' application on Host A might communicate with the 'REF' application on Host B.

3. Some applications have access to 'TEL' a telecommunications facility serving a local clientele. The local clientele is symbolized in the diagram by the antenna-like symbols. The applications available to the local clientele may differ from the ones that the same host makes available to the Network.

4. The juxtaposition of 'NET' and 'TEL' facilities with applications in the diagram does not indicate in any way that all these functions are carried out on any one single piece of hardware.

B. Network Model Assumptions

Several assumptions affecting protocol design have been made by the Task Force.

At the application level, messages will not be forwarded from process to process or host to host. A message will go from a single host on the Network to another host and the response will return to the originating host. If the host that received the request cannot respond to the request it will inform the originating host. It will be the originating host's responsibility to retransmit the request to another host on the Network, if desired. The complexity of message forwarding (that is, having the first target host pass the message on to a third host which would respond directly to the originating host) cannot be justified by the possible reduction of message traffic. The transaction-forwarding mechanism would cost more in header and protocol complexity, data space, etc., than would be saved by reduced message traffic.

The Task Force also has assumed that the protocol will not address the area of standard command formats and structures such as standard search queries, error messages, and cataloging commands. Most likely, host processes will have differing commands. Therefore, some translating or reformatting of requests will be necessary. Translation could occur in any one of three ways: 1) The end user at the terminal could re-input the request in the format required by the remote host; 2) the local host automatically could translate the request into the required formats; 3) the local host automatically could translate the request into a Network standard format, which would in turn be translated by the remote host into its internal format. In the long run the third approach is preferable, but in the absence of necessary command standards, the application protocol will allow all three methods to be implemented.

The Network protocols will be based on the "layered" concept (Figure III.1, Page 8) in which protocol levels or "layers" can be identified and independently described and implemented. If independence between layers is achieved, the protocols at individual layers can be changed with minimal effect on other layers. Much previous work has already been done in the standard lower-level protocols (network level, link level, etc.). The present work addresses the higher level "application level" protocol. The application level protocol is independent of the physical nature of the communications subnetwork which provides reliable communications between hosts on the Network.

C. Application Transactions

The Network will transmit messages to support various library applications processes. Figure IV.2 noted several applications processes, including acquisitions, cataloging, circulation, reference and serials control.

The acquisitions process involves the ordering and processing of books from vendors and other sources. Typical transactions that could occur in this process include: pre-order searching of

bibliographic data; citation verification; transmitting orders electronically to vendors; transmitting claim and cancellation notices to vendors in the event of non-delivery of material; transmitting requests for quotations on rare or out-of-print materials and sending subsequent orders; transmitting on-line invoices and accounting information to ordering institutions (by vendors); and transmitting information regarding an order, including cancellations and delayed notations to acquiring libraries or to their representative service centers (by vendors). A single library acquisitions activity may cause several transactions in sequence (e.g., a pre-order search followed by an order).

Cataloging process transactions include: searching for bibliographic data for cataloging; distributing records cataloged at one service center to other service centers for inclusion in the target centers' data bases; ordering various cataloging products such as catalog cards, book and microform catalogs, and transmitting data useful for the production of these products; and maintaining authority control transactions which would reference an authority source on the library network for validating input data.

The circulation and interlibrary loan (ILL) process transactions include: searching for citation verification; locating a library which holds a particular citation; verifying the availability of an item; and transmitting a request for the item. Since in the future patrons may attempt to borrow items at a library other than their home libraries, cross-checking a patron's status through the Network might be required.

The reference process includes those transactions which are typically performed at a reference desk in the library. These include searches for citations and requests to abstracting and indexing services.

Serials control, a special subfunction of acquisitions, includes the following transactions: ordering serials; renewing serials orders; claiming and cancelling serials orders and particular items; verifying the arrival of certain serials; and union catalog postings. The union catalog postings would be similar to the record distribution transactions mentioned under cataloging, for updating serials holdings in various union catalogs.

Certain direct user-service transactions could also occur. These include searches for specific items; bibliography requests; establishment of selective dissemination of information (SDI) profiles; and distribution of SDI records. In addition, certain user-service transactions could occur that do not map neatly into standard library functions. These include message handling for transmission of information concerning the Network or the hosts connected to the Network. The type of information transmitted might pertain to statistical and network accounting data, or to

batch billing data and invoices for network services (as distinguished from services provided by the individual entities).

Certain control type messages will maintain the integrity of interprocess transactions. These include availability checks, session establishment messages, application error checking and traffic loading statistics.

A summary of the applications and functions discussed above is presented in Table IV.3.

D. Transaction Message Flows

A study of message flow to support the above functions indicates that six basic types of transaction flow can be identified. Table IV.4 outlines these six types of transaction flow. The six types support all of the functions previously discussed. For example, the reference function would probably use Request/Response pairs for search transactions; the cataloging function may use Request/Response pairs for pre-catalog searching and then Message/Acknowledgement pairs for cataloging input.

E. Registry

In the course of its deliberations, the Task Force expanded on the "registry" concept outlined by ISAD/TC. The Registry will serve two distinct functions for the Network protocol: 1) It will function as a depository for the current up-to-date and correct version of the protocol; 2) it will be responsible for assignment of Field Identifiers (FID's) and Field Values (FV's). FID's and FV's are defined in detail in Section V.

The Task Force anticipates that several refinements, changes and enhancements will be made to the protocol during its implementation. As the protocol is implemented, the Task Force expects hosts to request that additional header fields be added. The Registry will record all additions and changes and will insure their consistency with the rest of the protocol. In addition, the Registry will validate all meanings and values of the FID's and FV's. These components are present in all header fields. If the protocol is to be useful, header field meanings must be both accepted and understood by all hosts.

The Registry's responsibility for assignment of new FID's and FV's can be likened to the position of a "data base administrator." "Requests for new assignments" will be directed to the Registry which will in turn check the requests against existing items to avoid duplications and maintain consistency.

Table IV.3: FUNCTIONS AND TRANSACTIONS

ACQUISITIONS

- Preorder searching
- Orders to vendors
- Claims/cancel notice
- Search/quote
- On-line invoicing/accounting
- Vendor cancel

CATALOGING

- Searching
- Distribution of records
- Product order
- Authority control check

CIRCULATION/INTERLIBRARY LOAN

- Searching
- ILL availability check
- ILL request
- Patron check

REFERENCE

- Searching
- Transparent request to abstracting and indexing service

SERIALS CONTROL

- Claim/cancel
- Renewal
- Order
- Arrival check
- Union Catalog

USER SERVICE

- Searching
- Bibliography request
- SDI profile
- SDI record distribution

OTHER SUPPORT

- Message switching
- Statistical reports
- Network accounting
- Transparency
- Bill service

CONTROL

- System/process availability
- Load statistics
- Reliability checks
- Error reporting

Table IV.4: TRANSACTION FLOW

	Originating Host	Target Host
1. Message (Unacknowledged)	Message ----------→	
2. Message/Acknowledgement	Message ----------→ Acknowledgement ←----------	
3. Request/Response	Request ----------→ Response ----------	
4. Request/Acknowledgement/ Delayed Response	Request ----------→ Acknowledgement ←---------- (Time Delay) Response ←----------	
5. Request/Multiple Response	Request ----------→ Response ←---------- Response ←---------- Response ←----------	
6. Request/Response/ Request for More	Request ----------→ Response ←---------- Request for More ----------→ Response ←---------- Request for More ----------→ Response ←----------	

V. PROTOCOL

A. Terminology

The terminology used in this paper is defined in Appendix C. Where possible, words and meanings currently accepted as standards are used in the discussions. However, inconsistencies with previous terminology may occur in that several new concepts have been introduced.

B. Protocol Assumptions

The Task Force has made several assumptions about the nature of the Network protocol. These assumptions are as follows:

1. Although the protocol generally is symmetrical in that it provides for bidirectional communication, certain concepts surrounding the roles of 'originating' and 'target' hosts make that relationship asymmetrical. It should be noted that services are being supplied to the originating host by the target host. Under the assumption that money flows in the opposite direction from services, all billing and accounting responsibilities lie with the target host.

   It is conceivable that some activities, such as mutual exchange of files, would result in services being provided in both directions. Consequently, there would be a need for billing in both directions. One possible solution to this problem would be to establish two different sessions simultaneously for this kind of application.

2. The protocol is oriented primarily toward maintaining the orderly flow of on-line interactive information. However, bulk transfer of data, especially file transfers, can be accommodated by adding application level logic to control the process. This problem was not studied in any detail by the Task Force and should be addressed at a future time.

3. Some national and/or international standards underlie the protocol described herein and provide for an error-free subnetwork or medium for the delivery of information. The Task Force assumes that this subnetwork will deliver all messages in their proper sequence. Some flow control, or 'backpressure', is provided by the protocol at the application level on a session-by-session basis but no counterchecking

of the communications network or of the integrity of the subnetwork is provided by this protocol.

4. Regardless of the actual topology of the communications subnetwork, communication at the application level occurs on a point-to-point basis between any two host computers. The Network therefore gives the appearance of being totally connected.

5. Hosts are not expected to 'forward' messages to other hosts and there is no 'broadcast' facility which might allow for a message to be sent to all other hosts.

6. Although it is conceivable that an intelligent terminal might be programmed to implement the protocol, it has not been the intent of the Task Force to address the question of terminal protocols. It is expected that only major host facilities will be connected to the Network via conventional telecommunications monitors or similar means.

C. Message Classes

Two distinct classes of messages will support the variety of functions and purposes projected within the Network: control messages and data messages.

A message is a unit of information (i.e., a sequence of bits) transmitted from one host to another host on the Network. It serves as the medium of exchange of data and control information between communicating hosts.

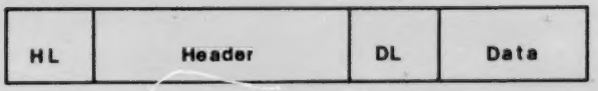
As implied by its name, a control message manages, supervises and coordinates the message flow at the application levels between two communicating hosts. Control is necessary at both a message and a session level. Control messages can be used to begin and control a session, and invoke and control application functions.

A session constitutes an association between a process at one host and a process at another host through a sequence of control messages exchanged between the hosts. Sessions must be initiated and ended explicitly via an exchange of control messages. The host that begins the session is designated the originating host; the host with which the originating host wishes to communicate is designated the target host. A session initiation may be viewed as an application level "log-on" and process selection procedure. This procedure serves to inform the target host which process the originating host wishes to invoke and establishes a billing account code for the target host to use. Any host in the Network can establish a session with another host, or multiple sessions with one or more hosts.

Data messages are simply messages not defined as control messages. Generally, data messages contain the basic elements of information pertinent to the proper execution of an application function executing at a target host on behalf of an originating host.

D. Message Format

All Network messages will have the following format:



where:

HL is the length of the header that follows. It is two octets long and contains a binary integer.

Header includes the various header fields required for this message.

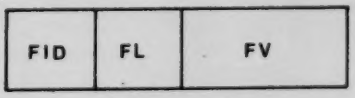
DL is the length of the data that follow. It is two octets long and contains a binary integer. If there are no data associated with the message, this field contains binary zeroes.

Data are the various data fields transmitted by the sender of the message.

The header is broken down into header fields as shown in Figure V.1, Page 24.

Note that in the diagram, no order is implied in the order of header fields. The number of header fields can vary, as will be explained in this section.

The component parts of all header fields are: Field IDentification (FID), Field Length (FL), and Field Value (FV).



where:

FID is the unique binary value one octet in length used to identify the field.

FL is the binary value, one octet in length, specifying the number of octets taken up by the following field value.

FV is the data identified by the FID.

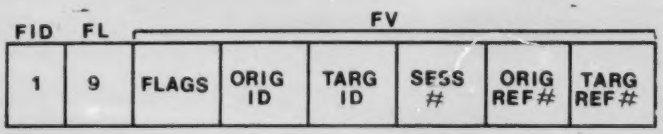
The field identification alone may be sufficient to process the field. In this case there is no field value. If there is no field value, the field length is set to zero.

E. Required Header Fields

Two header fields are required in all messages: the Address/Reference Field and the Message Type Field. Other header fields may be required depending on the field value of the Message Type Field.

1. Address/Reference Field

The format of the Address/Reference Field is as follows:



where:

FLAGS is one octet long. The meaning and use of each bit are illustrated in Table V.2 on Page 25.

ORIG ID is a 16-bit binary number that uniquely identifies the originating host in the Network. The value is obtained from the Network Registry.

TARG ID is a 16-bit binary number that uniquely identifies the target host in the Network. The value is obtained from the Network Registry.

SESS # is a 16-bit binary number assigned to the session by the originating host.

ORIG REF # is an eight-bit binary reference number assigned and controlled by the originating host.

TARG REF # is an eight-bit binary reference number assigned and controlled by the target host.

The Address/Reference Field is used to route messages at the application level. This field differs from the one required by the communications subnetwork. The ORIG ID, TARG ID, and SESS # portions of this field serve uniquely to identify a session between hosts.

The originating host is the host that sends the Begin Session Message. The target host is the host that receives the Begin Session Message. This identification is retained throughout the session. Note: Flag bit 1 identifies for each message whether the originating host is the source or destination of the message.

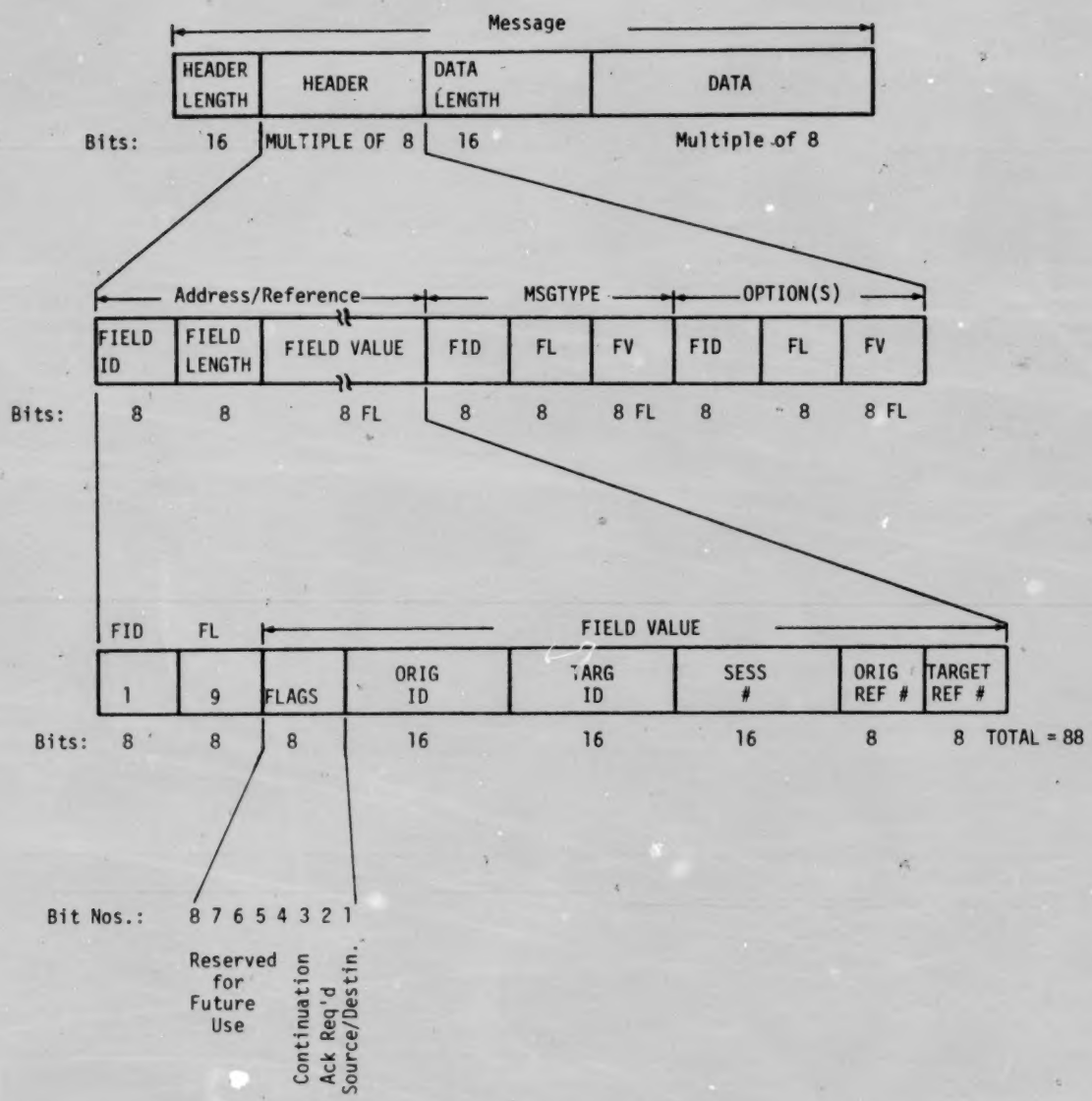


FIGURE V.1: DETAILED MESSAGE STRUCTURE

Table V.2: FLAG BITS AND MEANINGS

Bit	Meaning
1	Source/Destination Indicator: If the source of the message is the originating host, the bit is set to zero. If the destination of the message is the originating host, the bit is set to one.
2	Acknowledgement Required Indicator: If the source host requires an acknowledgement to the message from the destination host, the bit is set to one. (The acknowledgement will be sent via an Acknowledgement Message.) If the bit is set to zero, no acknowledgement is required. A more detailed discussion of Acknowledgement Messages is presented in this chapter.
3	Continuation Indicator: When this bit is set to one, the source host has additional messages associated with this transaction to send to the destination host. The source host will therefore be the "sender" of the next non-control message of the session. If this bit is set to zero, the source host has no additional data messages to send. The Continuation Indicator has meaning only within a data message.
4-8	Reserved for future use.

The destination host's last reference number is repeated in the source host's next message. When an originating host sends a message to a target host, it inserts the target host's reference number in the TARG REF # Field. At the same time, the originating host assigns a number to its own reference field, the ORIG REF # Field.

When the target host receives the message, it uses the originating host's reference number in the message it returns, the same as above. That is, when the target host sends back a message, it takes the originating host's reference number and inserts it in the ORIG REF # Field. As above, the target host assigns a reference number to itself and places the number in the TARG REF # Field. This process is illustrated in Figure V.3 below.

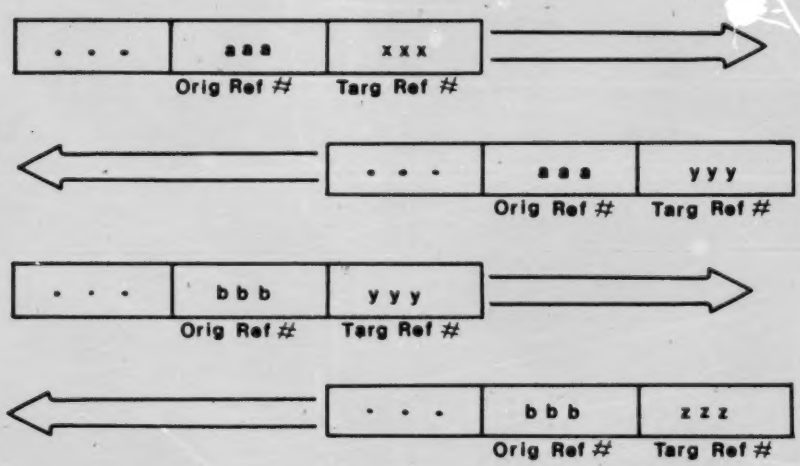


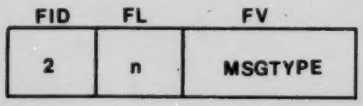
Figure V.3: USE OF REFERENCE NUMBERS

The value zero may be used at any time by any host as its reference number. In addition, the value zero must be used as the target host's reference number for a Begin Session Message.

Within application-to-application communications, the reference numbers appear to be arbitrarily assigned. However, a host's reference number probably will be meaningful to the host itself. A given host can parse its reference number into several small parts to route received messages to the proper application and to help maintain an orderly internal environment.

2. MeSsaGe TYPE

The format of the Message Type Field is as follows:



where:

MSGTYPE is a number uniquely identifying the type of message being sent.

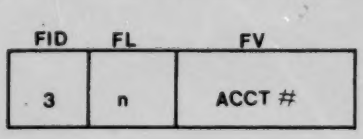
The value of the MSGTYPE Field determines whether additional header fields are required. Possible values of the MSGTYPE Field are discussed in detail under "Control Messages" and "Data Messages" in this section.

F. Optional Header Fields

The type of control message being sent will determine which optional header fields are required. Furthermore, certain control messages will cause some optional header fields to be illegal fields. Optional header fields are defined here. The next subsection, "Control Messages", further defines the requirements for these fields.

1. ACCounT Number

The format of the Account Number Field is as follows:



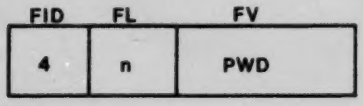
where:

ACCT # is the billing account code used by a target host to charge for its services. There may be more than one account number for a host. The Task Force recommends that a standard

account number format be developed and that account numbers be registered.

2. PassWorD

The format of the Password Field is as follows:

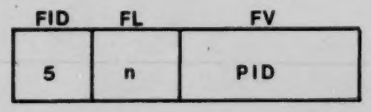


where:

PWD is the password the target host requires to assure some degree of security. PWD Field contents, of course, are not registered but rather arrived at via bilateral agreements between hosts.

3. Process IDentification

The format of the Process Identification Field is as follows:

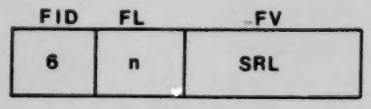


where:

PID is the Process Identification Field that identifies the process invoked at a target host by an originating host. The PID Field contains a registered binary value which identifies a process (e.g., cataloging, acquisitions, etc.).

4. Session Resource Limit

The format of the Session Resource Limit Field is as follows:



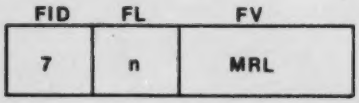
where:

SRL is the maximum amount of money an originating host will spend during the session. The SRL Field contains a binary number specifying the amount in U.S. cents. Although this field may be sent to a target host, not all target hosts will be able to calculate billing charges dynamically.

In this case, an Exception Message will be generated.

5. Message Resource Limit

The format of the Message Resource Limit Field is as follows:

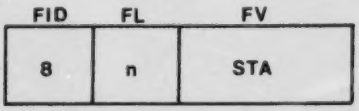


where:

MRL is the maximum amount of money an originating host will spend during the processing of a single message. This value should not be greater than the amount of the Session Resource Limit left for a session. If it is greater, the amount of the remaining Session Resource Limit is used. The MRL Field contains a binary number specifying the amount in U.S. cents. Again, although this field may be sent to a target host, not all target hosts will be able to calculate billing charges dynamically. In this case, an Exception Message will be generated.

6. STAtus

The format of the Status Field is as follows:

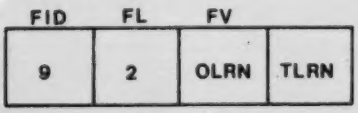


where:

STA is the status of the current session and/or last message. The field contains a binary number which defines the status. The meanings of the possible field values are registered. The STA Field serves as the vehicle for transmitting errors detected by the applications and is repeatable within the header. (See Exception Message Type.)

7. Last RefereNce

The format of the Last Reference Field is as follows:



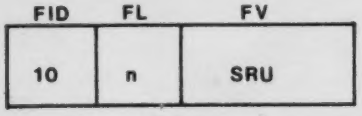
where:

OLRN is the Originating host's Last Reference Number sent on the last data (i.e., non-control) message of the session.

TLRN is the Target host's Last Reference Number sent on the last data (i.e., non-control) message of the session.

8. Session Resources Used

The format of the Session Resources used field is as follows:

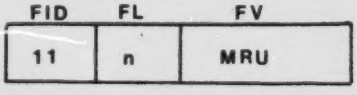


where:

SRU is the value of the resources used to process the current or last session. The SRU Field contains a binary number representing the approximate charge incurred in U.S. cents. Although this field is defined, not all hosts will be able to furnish the data dynamically.

9. Message Resources Used

The format of the Message Resources Used Field is as follows:

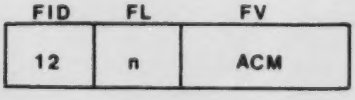


where:

MRU is the value of the resources used to process the current or last message. The field contains a binary number representing the approximate charge incurred in U.S. cents. Although the MRU Field is defined, not all hosts will be able to furnish this data dynamically.

10. ACcounting Method

The format of the Accounting Method Field is as follows:



where:

ACM is a number which indicates the desired accounting algorithm for figuring the cost of the session. The values of this field will be registered in the Registry. Examples of uses of this field include bulk discounts, special service modes, etc.

11. Date and Time Stamp

The format of the Date and Time Stamp Field is as follows:

FID	FL	FV
13	15	DTS

where:

DTS is the date and time stamp in the format YYYYMMDDHHMMSSZ, where YYYY is the year, MM is the month, DD is the day, HH is the hour, MM is the minute, SS is the second and Z indicates the Coordinated Universal Time (or Greenwich Mean Time). This format is in accordance with ISO standard ISO 3307-1975(E).

12. Data Format

The format of the Data Format Field is as follows:

FID	FL	FV
14	n	DF

where:

DF is the format of the data in the data portion of the message. Examples of formats might include MARC Books Format, MARC Serials Format, "3,3 key," detailed status format, and number or number string. When a format is registered, a list of allowable data codes must be registered; also, a default data code should be registered.

13. Data Code

The format of the Data Code Field is as follows:

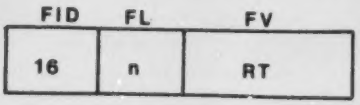
FID	FL	FV
15	n	DC

where:

DC specifies the coding convention used in the data portion of the message. The data code values must be registered. Examples of data codes include ASCII and EBCDIC for character data, and binary and packed decimal for numeric data.

14. Response Type

The format of the Response Type Field is as follows:

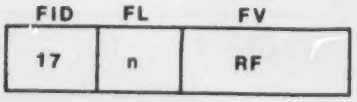


where:

RT represents the desired message type for response to the message in which this field occurs. This field allows a host to insure that the response is the type desired. For example, a host could request a count of the records retrieved as the result of a search or could request that the records be sent directly. If the destination host cannot supply the desired message type, an Exception Message will be returned. The message types for this field are the same as for the Message Type Field except that only data message types may be requested in this field.

15. Response Format

The format of the Response Format Field is as follows:



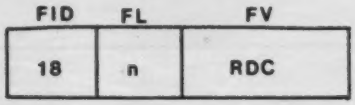
where:

RF is the response format a host wishes to receive for the data portion of the response to a message. The RF Field insures that the response a host gets is in a format which it can handle. If the destination host cannot supply the requested format, an Exception Message should be generated to inform the host of this. The format

types are the same for this field as for the Data Format Field and are registered as such.

16. Response Data Code

The format of the Response Data Code Field is as follows:

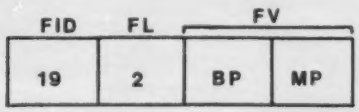


where:

RDC specifies the coding convention used in the data portion of the Response Message. This field ensures that a host will be able to process the response to the message. If the destination host cannot supply the requested code, then an Exception Message will be generated. The numeric codes used in this field are identical to those used in the Data Code Field and must be registered.

17. Priority

The format of the Priority Field is as follows:



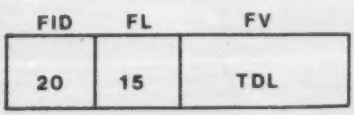
where:

BP is the Base Priority indicating the initial priority used in processing this message. This octet contains a binary number from Ø to 255. Zero is the lowest priority and 255 is the highest priority. Priority is meaningful only to the target host and is host-dependent.

MP is the Maximum Priority and indicates the maximum level to which the priority may be raised to achieve the time limit requested. The MP octet contains a binary number from Ø to 255 where Ø is the lowest priority and 255 is the highest priority.

18. Time DeadLine

The format of the Time DeadLine Field is as follows:



where:

TDL is the time and date in the format YYYYMMDDHHMMSSZ (ISO 3307-1975E) when processing of the message is to be completed. If the message processing is not completed by that time, a Suspend Message (see "Control Messages") should be sent. Priorities may be adjusted upward to the maximum priority to meet the deadline specified. Not all systems will be able to honor time deadline requests. In this case, an Exception Message will be generated.

G. Control Messages

Control messages help manage and coordinate communication at the application level between two hosts. Depending on the type of control message being sent, some of the previously-defined optional header fields become required fields. This section details the types of control messages that can be sent, when they are sent, and the action(s) which must be taken upon their receipt. Required and optional header fields are noted for each type of control message. Possible responses to the control messages also are listed where applicable.

1. Begin Session

Contents of Message Type Field:

FID	FL	FV
2	1	1

When Sent:

A Begin Session Message is sent by an originating host to a target host to select a process at the target host (e.g., cataloging, acquisitions, etc.).

Action Upon Receipt:

When the target host receives the message, it establishes a context area for the session and sends a Begin Session Response Message to the originating host.

Required Header Fields:

1. Address/Reference
2. Message Type
3. Process Identification
4. Account Number

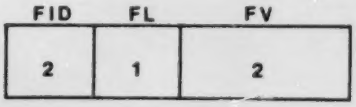
Optional Header Fields:
1. Password
2. Session Resource Limit
3. Date and Time Stamp
4. Priority
5. Accounting Method

Possible Responses:
1. Begin Session Response
2. Inappropriate Response
3. No Response

The expected response to this message is a Begin Session Response Message. The Begin Session Response Message indicates that the target host either is or is not prepared to provide the process requested via the Process Identification Field. A "no response" or "inappropriate response" indicates an error has occurred and some sort of application level error recovery should be attempted. If the Session Resource Limit Field is omitted, the target host can assume that no resource limit should be established.

2. Begin Session Response

Contents of Message Type Field:



When Sent:

A Begin Session Response Message is sent by a target host in response to an originating host's Begin Session Message.

Action Upon Receipt:

The originating host examines the Status Field of the Begin Session Response Message to determine if the target host is prepared to provide the requested process. A non-zero status value indicates that the target host has denied the originating host access to the requested process. The value of the Status Field contains a registered code which explains the reason for the denial.

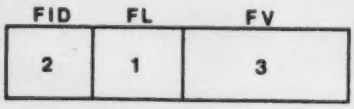
Required Header Fields:
1. Address/Reference
2. Message Type
3. Status

Optional Header Fields:
1. Process Identification
2. Date and Time Stamp

The Begin Session and Begin Session Response Messages confirm that the process is available and that both hosts have correctly initiated the session.

3. End Session

Contents of Message Type Field:



When Sent:

An End Session Message is sent by an originating host to a target host to end a session.

Action Upon Receipt:

The target host upon receipt of an End Session Message determines if a session can be ended. A session cannot be ended if the target host is processing a message for the session from the originating host. An End Session Response Message is always sent.

Required Header Fields:
1. Address/Reference
2. Message Type

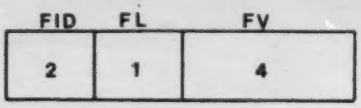
Optional Header Fields:
1. Process Identification
2. Date and Time Stamp

Possible Responses:
1. End Session Response
2. Inappropriate Response
3. No Response

An End Session Response Message indicates that the target host either has or has not ended the session. Both the "no response" and the "inappropriate response" indicate an error has occurred and some sort of application level error recovery should be attempted.

4. End Session Response

Contents of Message Type Field:



When Sent:

An End Session Response Message is sent by the target host to the originating host in response to the originating host's End Session Message.

Action Upon Receipt:

The originating host examines the Status Field of the End Session Response Message to determine if the target host has ended the session. A non-zero Status Field value indicates the target host has not ended the session. The Status Field value contains a registered code which explains the reason that the session was not ended.

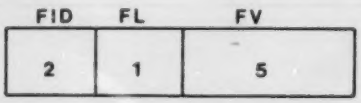
Required Header Fields:
1. Address/Reference
2. Message Type
3. Status

Optional Header Fields:
1. Session Resources Used
2. Date and Time Stamp

A response is not required for this message as the termination of the session has been requested by the originating host and verified, or rejected, by the target host.

5. Status Query

Contents of Message Type Field:



When Sent:

A Status Query Message is sent by either an originating host or a target host to determine the current status of another host regarding an in-process session.

Action Upon Receipt:

When a host receives a Status Query Message,

it sends a Status Query Response Message which details its current processing state.

Required Header Fields:
1. Address/Reference
2. Message Type

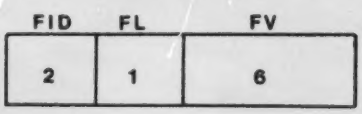
Optional Header Fields:
1. Date and Time Stamp

Possible Responses:
1. Status Query Response
2. Inappropriate Response
3. No Response

The expected response to a Status Query Message is a Status Query Response Message which details the current status of the queried host. An "inappropriate response" or "no response" indicates an error has occurred and some sort of application level error recovery should be attempted.

6. Status Query Response

Contents of Message Type Field:



When Sent:
A Status Query Response Message is sent by a host in response to a Status Query Message from another host.

Action Upon Receipt:
The host that receives the message examines the various header fields sent with the Status Query Response Message. Based upon this examination, the receiving host takes whatever action is necessary.

Required Header Fields:
1. Address/Reference
2. Message Type
3. Last Reference
4. Account Number
5. Process Identification
6. Status

Optional Header Fields:
1. Date and Time Stamp
2. Session Resources Used
3. Message Resources Used
4. Priority
5. Time Deadline

The Status Field of a Status Query Response Message indicates the source host's determination of its current processing state for the current session/message. The value of the Status Field is a registered code that reflects the source host's determination.

7. Purge Message

Contents of Message Type Field:

FID	FL	FV
2	1	7

When Sent:

A Purge Message may be sent by any host to terminate processing of a data type message.

Action Upon Receipt:

When a host receives a Purge Message, it immediately terminates processing of any data type messages currently active for the session. Also, any unsent messages for the session are cleared and are not transmitted.

Required Header Fields:
1. Address/Reference
2. Message Type

Optional Header Fields:
1. Date and Time Stamp

Possible Responses:
1. Purge Message Response
2. No Response
3. Inappropriate Response

The expected response to a Purge Message is a Purge Message Response Message. The Purge Message Response Message details the action taken by the destination host. Both the "no response" and the "inappropriate response" indicate that an error has occurred and some type of application level error recovery procedures should be invoked.

8. Purge Message Response

Contents of Message Type Field:

FID	FL	FV
2	1	8

When Sent:
A Purge Message Response Message is sent in response to a Purge Message.

Action Upon Receipt:
A host receiving a Purge Message Response Message examines the Status Field of the message to determine what action was taken by the source host. A zero value Status Field indicates that the message and any untransmitted responses were cleared. A non-zero value indicates the message and any untransmitted responses were not cleared. The Status Field value is a registered code which indicates the reason items were not purged.

Required Header Fields:
1. Address/Reference
2. Message Type
3. Status

Optional Header Fields:
1. Date and Time Stamp
2. Message Resources used

9. Purge Session

Contents of Message Type Field:

FID	FL	FV
2	1	9

When Sent:
A Purge Session Message may be sent by either an originating host or target host whenever it wishes the destination host to terminate immediately an in-process session without transmitting, retaining, or receiving any unsent responses for unprocessed messages associated with the session.

Action Upon Receipt:
If the destination host is the originating host, it clears its session level context area and no longer expects to receive any messages from the target host for this session. If the destination host is the target host, it treats the message as if it were an End Session Message except that it immediately clears any unsent or unprocessed control or data messages.

Required Header Fields:
1. Address/Reference
2. Message Type

Optional Header Fields:
1. Date and Time Stamp
2. Session Resources Used
3. Status

Possible Responses by Target Host:
1. End Session Response
2. No Response
3. Inappropriate Response

Possible Responses by Originating Host:
1. None

If the originating host is the source of the Purge Session Message, the expected response is an End Session Response Message that details what action was taken by the target host and includes system resource utilization figures.

10. Acknowledgement

Contents of Message Type Field:

FID	FL	FV
2	1	10

When Sent:

An Acknowledgement Message is sent by either host whenever it receives a message that has the Acknowledgement Required bit in the Address/Reference Field set to one. The only exception to this is an Acknowledgement Message itself. Even if the Acknowledgement Requested bit is "set" in an Acknowledgement Message, no Acknowledgement Message is sent.

Action Upon Receipt:

The destination host of an Acknowledgement Message takes whatever internal action is required upon receipt of the Acknowledgement Message.

Required Header Fields:
1. Address/Reference
2. Message Type

Optional Header Fields:
1. Date and Time Stamp

An Acknowledgement Message indicates to the destination host that the previous message it sent was received, the Address/Reference Field is valid, and the message type is not an Acknowledgement. An Acknowledgement Message in no way implies

anything about the validity of the remaining fields. To avoid a loop, an Acknowledgement Message may not request an Acknowledgement Message.

11. Exception

Contents of Message Type Field:

FID	FL	FV
2	1	11

When Sent:

An Exception Message is sent by either an originating host or a target host whenever it detects an unusual or exceptional condition as a result of, or as a by-product of, processing a message from another host.

Action Upon Receipt:

A host examines the Status Field value to determine the cause of the exception. The Status Field contains a registered binary code which indicates the reason for the exception. After diagnosing the reason for the exception, the destination host takes whatever action (corrective or abortive) is necessary to relieve the condition.

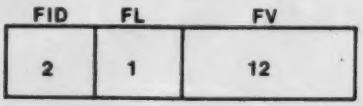
Required Header Fields:
1. Address/Reference
2. Message Type
3. Status

Optional Header Fields:
1. Date and Time Stamp

A host should be prepared at all times to receive an Exception Message as a result of any message it may send. Exception Messages may be initiated by such diverse events as a resource limit exceeded, an invalid header field value, invalid data in a data field, etc. An Exception Message can even be received for another Exception Message. The required remedial action is completely dependent on the cause of the exception. Some possible actions to remedy the exception are to send a Status Query Message, Purge Session Message, or Purge Message; reformat a message; revalidate header field values, etc. Although an Exception Message has not been listed as a possible response for other control messages, it is always a possible response, albeit a rare occurrence.

12. Suspend

Contents of Message Type Field:



When Sent:

A Suspend Message may be sent by a source host to inform the destination host that it has temporarily ceased processing a message pending further information from the destination host.

Action Upon Receipt:

The destination host examines the Status Field to determine the cause of the suspension. The Status Field contains a registered code which explains the cause of the suspension.

Required Header Fields:
1. Address/Reference
2. Message Type
3. Status

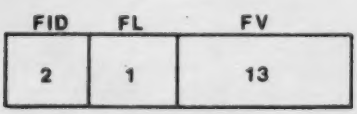
Optional Header Fields:
1. Date and Time Stamp

Possible Responses:
1. Resume
2. Purge Message
3. Inappropriate Response
4. No Response

A Suspend Message indicates that the source host is awaiting further information and/or clarification from the destination host (in the form of a Resume Message) before processing can continue. A possible cause of a Suspend Message might be that the message resource limit has been exceeded. Both the "no response" and "inappropriate response" indicate that an error has occurred and that some sort of application level error recovery procedures should be invoked.

13. Resume

Contents of Message Type Field:



When Sent:
A Resume Message may be sent as a response to certain Suspend Messages. Any Suspend Message that has a Status Field value which indicates that the host has temporarily suspended processing of a message pending further clarification/instruction may result in a Resume Message.

Action Upon Receipt:
A target host examines the header and/or data fields of the received Resume Message to determine if sufficient information is present to continue processing the suspended request. If sufficient information is available, the host resumes processing. If it is not available, other recovery and/or termination action(s) should be initiated.

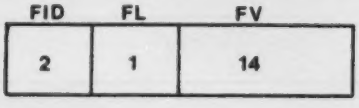
Required Header Fields:
1. Address/Reference
2. Message Type
3. Other Header Fields depending on the cause of the suspension

Optional Header Fields:
1. Date and Time Stamp

The header fields required in a Resume Message are determined by the cause of the suspension. For example, if a request was suspended because the message resource limit has been exceeded, the Message Resource Limit Field would be required to indicate to the target host an additional message resource limit value.

14. Wait

Contents of Message Type Field:



When Sent:
A Wait Message is sent by a source host when it wants to signal the destination host to stop sending messages.

Action Upon Receipt:
A host that receives a Wait Message immediately stops sending messages to the source host for the session. This does not imply that the destination host should stop processing messages for this session.

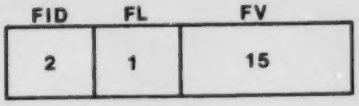
Required Header Fields:
1. Address/Reference
2. Message Type

Optional Header Fields:
1. Date and Time Stamp

The Wait Message is treated as an "out of band" signal since it receives priority over any other session message. A Wait Message must be processed and heeded in a timely manner as it implies the source host has encountered some sort of internal stress and/or difficulty. Further, receipt of messages may jeopardize the source host's ability to continue message processing. A host must be prepared to receive and act upon a Wait Message at any time after a session has begun.

15. Continue

Contents of Message Type Field:



When Sent:
A host sends a Continue Message when the internal condition which previously caused it to send a Wait Message has been alleviated.

Action Upon Receipt:
A host receiving a Continue Message immediately sends any messages it has queued for the session.

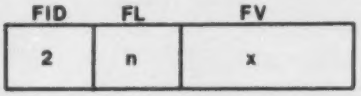
Required Header Fields:
1. Address/Reference
2. Message Type

Optional Header Fields:
1. Date and Time Stamp

A Continue Message inplies that the stressful condition at the source host has been eased and that the source host is again able to receive and process messages for the session.

H. Data Type Messages

Data type messages carry the actual information (request, response, etc.) of the work to be done. The format of the Message Type Field is as follows:



The Address/Reference Field and Message Type Field are the only fields required in data type messages. The Address/Reference Field is used in the same way as in control messages except for the Continuation Indicator (Table V.2, page 25).

If the Continuation Indicator Flag bit is set, it implies the source host intends to send another message prior to a response (except possibly for an Acknowledgement Message).

The Message Type Field contains a number which indicates the type of message contained in the data portion of the message. Message types are registered in the Registry whenever two or more hosts on the Network agree to use a new message type. Data message types have a default data format and a list of allowable message formats associated with them and registered in the Registry. Examples of data message types include search, response count, order, interlibrary loan request, and bibliographic record.

Data type message headers may include optional fields such as Data Format, Data Code, Response Format, Response Code, Message Resource Limit, Priority, Time Deadline, Date and Time Stamp, and Resources Used.

Any type of message may be used in response to a data type message except Begin Session, Begin Session Response, Purge Message Response, End Session Response, Status Query Response and Purge Session Response.

VI. SUMMARY AND RECOMMENDATIONS

In several ways, this report raises as many questions as it answers. It was not possible for the Task Force to address all of the questions concerning the Network protocol during its work. Therefore, the Task Force has enumerated eight specific recommendations for further study.

1. The responsibilities of the Registry must be defined and documented. The Registry itself must be established. There must be a clear understanding of the Registry's operation and how it interacts with the Network.

2. A study should be conducted to determine operational requirements of the Network using this protocol. The study should explore organizational as well as technical details, especially in the areas of responsibility for troubleshooting, maintenance, billing, accounting, etc.

3. The protocol will inevitably need modifications and enhancements once it is implmented and operational. An on-going committee should be formed to act as a continuing forum for discussion and review, and to provide an orderly mechanism for change.

4. Standardization of message content will be an important issue for the useful implementation of the protocol on a nationwide basis. Such standardization will also be very useful for initiating the Registry. The Task Force recommends that further work be done in this area.

5. Very little is said in this document about error recovery procedures, deadlocks, exceptions or other pathological problems. These areas should be explored and categorized. Once this is done, various unusual situations which could arise once many hosts are attached to the Network can be identified, documented and, where possible, resolved.

6. Investigation should be directed to the question of 'real time' as it applies to the protocols on the application level. Recommendations should be made as to acceptable time-out limits. In general, the relationship between the protocol and the communications subnetwork should be clarified.

7. The establishment of the protocol as a candidate standard through ANSI should be investigated. It is likely that the protocol will be of use outside the

library community. Attention should be given to disseminating the results of the work of the Task Force to other communities.

8. The protocol is, in some ways, a living entity and should not be allowed to lie dormant. Some effort should be devoted to implementing the protocol at several sites in order to prove its value and uncover any problems and difficulties. At the very least, organizations intending to implement the protocol should be encouraged to study it carefully with an eye toward uncovering problems specific to their operating system environment.

APPENDIX A: COMPOSITION OF THE TASK FORCE

The following members constituted the NCLIS/NBS Task Force on Computer Network Protocol:

TASK FORCE MEMBERS	TITLE/ORGANIZATION
Ruth L. Tighe Task Force Chairman	Research Associate, National Commission on Libraries and Information Science, Washington, D.C.
John L. Little Task Force Coordinator	Computer Specialist, National Bureau of Standards, Washington, D.C.
James K. Barrentine	Assistant Director, Research & Development Division, OCLC, Inc., Columbus, OH
Hanan S. Bell	Manager - Development, BALLOTS Center, Stanford University, Stanford, CA
David C. Hartmann	Senior Information Systems Analyst, Network Development Office, Library of Congress, Washington, D.C.
Nick A. Farmer	Development Projects Manager, System Development Department, Chemical Abstracts Service, Columbus, OH
James G. Hale, Jr.	Systems Support Officer, SADPO, New York Public Library, New York, NY
Clarice I. MacDonald	Supervisor for On-Line Information Systems, Boeing Computer Service, Seattle, WA
William D. Mathews	Director, Systems Division, New England Library Information Network, Wellesley, MA

COMMISSION REPRESENTATIVES

Andrew A. Aines NCLIS Commissioner	Senior Staff Associate, Division of Science Information, National Science Foundation, Washington, D.C.
Joseph Becker NCLIS Commissioner	President, Becker and Hayes, Los Angeles, CA
Alphonse F. Trezza NCLIS Executive Director	National Commission on Libraries and Information Science, Washington, D.C.

CONSULTANTS

Arthur J. Caisse	Tymnet Three Development Manager Tymshare Corporation, Cupertino, CA
John D. Day	Systems Analyst, Center for Advanced Computation, University of Illinois, Houston, TX
Philip L. Long	President, Philip Long Associates, Inc., Alexandria, VA
Jack Speer	Director of Library Information Services, Informatics, Inc., Rockville, MD
Barbara R. Sternick	Head, Data Communications Branch, National Library of Medicine, Rockville, MD
Barry D. Wessler	Director of Network Interfaces, Telenet Communications, Washington, D.C.
David Wolverton	Vice President for Administration, Brodart, Inc., Williamsport, PA

OTHER PARTICIPANTS

Henriette Avram	Special Assistant for Network Development, Library of Congress, Washington, D.C.
George E. Clark, Jr.	Acting Chief, Data Acquisitions & Storage Section, National Bureau of Standards, Washington, D.C.
Madeline Henderson	Chief, Computer Information Section, National Bureau of Standards, Washington, D.C.

Stephen R. Kimbleton	Chief, Computer Networking Section, National Bureau of Standards, Washington, D.C.
Albrecht J. Neumann	Computer Specialist, National Bureau of Standards, Washington,D.C.
Thomas N. Pyke, Jr.	Chief, Computer Systems Engineering Division, Institute for Computer Science & Technology, National Bureau of Standards, Washington, D.C.

APPENDIX B: AN EVALUATION OF LOWER LEVEL PROTOCOLS

In the data communications field, substantial work currently is being directed to specification, design, development, and implementation of computer communications protocols. The NCLIS/NBS Task Force on Computer Network Protocol is working on specifications for an application level (higher level) protocol for the transmission of messages between host computers in the Library and Information Services Network. The Task Force feels this application level protocol fits the conceptualization of layering of protocols. Therefore, it was decided that lower level protocols need not be addressed directly by the Task Force, but rather, certain of their capabilities should be assumed.

Protocols control data exchange, electrical signaling, timing, routing, data flow, error detection and correction, and status checking. By layering protocols, complex systems can be simplified through isolating individual functions. Layering of protocols also allows them to be implemented independently from one another in a separate layer or level. If complete independence is achieved between layers, standards can be developed for each layer and individual layers can be modified without affecting other layers. Each level may make use of the fact that functions are performed by lower levels and may perform functions that are, in turn, used by higher levels.

The concept of layering of protocols was presented in Chapter III. Lower level protocols which have been identified here include:

1) Hardware Level (between telecommunications equipment),

2) Link Level (between network switching processors),

3) Network Level (between network interface processors),

4) End-to-End Level (between host computers).

Protocols also exist between adjacent levels (e.g., End-to-end and Network Levels) to control level interfacing.

The NCLIS/NBS Task Force asked the National Bureau of Standards to evaluate current work in lower level protocols with respect to their application level work. The findings of NBS are summarized on the following pages.

Advantages and Disadvantages of Various Link-Level Protocols such as ADCCP (Advanced Data Communication Control Procedures), HDLC (High-Level Data Link Control), and SDLC (Synchronous Data Link Control), with respect to the work of the NCLIS/NBS Task Force.

The three link-level protocols ADCCP, HDLC, and SDLC are of identical genus. Although the specifications for the three protocols are structurally and editorially different, most of the components are consistently defined and technically compatible with each other.

The draft proposed ANSI standard for ADCCP is contained in a single document which prescribes three major subjects:

1. A frame structure enabling byte- and code-independent transmission that opens and closes with a flag sequence; contains an address, control, and frame check sequence; and may include an information field.

2. A command/response repertoire that may be signaled by control sequence I (information), N (numbered), or S (supervisory) encoding formats.

3. Several procedural classes, derived from three defined operational modes--asynchronous, normal, and balanced-- that may be implemented in corresponding link configurations which employ the unbalanced or balanced basic command/response sub-repertoires, each with up to nine operational functional extensions.

At its 1976 November meeting, ANSI Technical Committee X3S3 approved the forwarding of its ADCCP document X3S34/589/6 to X3 for consideration as an ANSI standard. The document should be available for X3 letter ballot during the Spring of 1977.

By contrast to the single document draft ANSI standard, the presently approved and draft proposed ISO standards that collectively prescribe High-Level Data Link Control (HDLC), address the above three standards but are contained in four documents. These documents are:

1. International Standard ISO 3309-1976, "High-level Data Link Control Procedures - Frame Structure."

2. Draft Proposed International Standard ISO DP 4335, "High-level Data Link Control Procedures -- Elements of Procedure (Independent Numbering)" that is presently the subject of an ISO/TC97 letter ballot.

3. Draft Proposed International Standard ISO/TC97/SC6-N1339, "High-level Data Link Control - Unbalanced Classes of Procedure" that is presently the subject of an ISO/TC97 letter ballot.

4. Draft Proposed International Standard ISO/TC97/SC6-N1340, "Balanced Classes of Procedure" that is presently the subject of an ISO/TC97/SC6 letter ballot.

SC-6 approved addendum and proposed enhancements for ISO DP4335 are contained respectively in documents ISO/TC97/SC6-N1300 and N1341.

Since considerable motivation exists for the ANSI standard to be compatible with the ISO standard, ADCCP is technically equivalent to HDLC in all important respects. In fact, portions of the ANSI document have been employed as the basis for developing much of the material contained in the separate ISO documents.

SDLC is the version of ADCCP/HDLC being implemented by IBM in its product lines. SDLC will be structured according to the IBM concept of System Network Architecture (SNA). The present version of SDLC, described in IBM publication GA27-3093-1, excludes several features specified for ADCCP such as the Asynchronous and Balanced Operational Modes. (This is not to suggest that IBM may not announce future enhancements of SDLC to bring it more into line with ADCCP.) The IBM publication also describes several features, e.g., NRZI signaling, that are not included in ADCCP. It is important to note that those subjects which are addressed by both SDLC and ADCCP appear to be technically consistent and therefore compatible.

Other manufacturers besides IBM also have announced products which implement ADCCP. The Burroughs version, called Burroughs Data Link Control (BDLC), claims full compatibility with ADCCP and HDLC. UNIVAC has announced a structured product line which employs its Distributed Communications Architecture (DCA). This architecture is similar to the IBM Systems Network Architecture concept. DCA will implement the link protocol, Universal Data Link Control (UDLC), in UNIVAC's version of ADCCP. (Attachment 1 from the December 1976 issue of Data Channels describes this UNIVAC announcement in some detail.)

Since ADCCP is being processed concurrently as a voluntary national standard and as a mandatory Federal Standard, it seems

appropriate for the NCLIS/NBS Task Force to consider employing ADCCP (as opposed to specifying any particular manufacturer's version of it, such as SDLC). The NCLIS/NBS Task Force should address the potential requirement for employing one or more of the various procedural classes prescribed by ADCCP. Even if network services for the library community will be procured from a carrier, the NCLIS/NBS Task Force should specify the terminal/network interface. On the other hand, the selection of a link level protocol should in no way affect the design of higher-level, applications-oriented protocols. Furthermore, there is no compelling reason why multiple link protocols could not be supported by a network on different access lines.

Present Controversy surrounding CCITT packet-switching standard X.25 with attention to the following:

* technical issues

* compatibility with other standards such as HDLC and X.21 (General Purpose Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment for Synchronous Operation on Public Data Networks)

* the necessity of end-to-end protocols in addition to the use of X.25.

CCITT Recommendation X.25 packet-switching standard (CNP-8) is organized into three separate levels of specification. These levels are:

1. The physical, electrical, functional, and procedural characteristics to establish, maintain, and disconnect the physical link between the Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE);

2. The link control procedure for data interchange across the link between the DTE and DCE;

3. The packet format and control procedures for the exchange of packets containing control information and user data between the DTE and DCE.

With respect to technical issues and compatibility with other standards, the unresolved technical issues involving X.25 are concerned with levels 2 and 3 above; level 1 specifies CCITT Recommendation X.21, and X.25 is compatible with X.21.

As of 1977 May, level 2 of X.25 is compatible with the ISO standards for HDLC; i.e., CCITT has essentially copied the relevant parts of the ISO frame structure standard (3309) and the elements of procedures standard (4335) into the X.25 document. However, initially in the process of writing X.25, CCITT prematurely selected a class of procedure for balanced, point-to-point link operations that was being proposed for adoption by ISO and which was, at the time, the subject of an ISO/TC97/SC6 letter ballot. A substantial majority of the respondents to the SC6 letter ballot (including the USA) recognized that this particular proposed class of procedure was technically deficient. As a consequence, the SC6 letter ballot failed and SC6 has since proceeded to develop an improved balanced class of procedure. Due to the uncoordinated and non-synchronized series of respective ISO and CCITT working group meetings and

approval processes, CCITT proceeded to approve X.25 in toto, as initially written. This led to a technically inconsistent application of HDLC and a point of incompatibility between ISO and CCITT. This situation was rectified during 1977 April both by ISO changing HDLC and CCITT changing X.25 so that they are now compatible.

The other presently unresolved technical issue concerned with level 3 of X.25 is that only a virtual call type packet network service capability has been specified. Various critiques insist that a datagram (single packet) type service capability is equally important. A consensus as to how this should be accomplished has not yet been reached.

With regard to the necessity of end-to-end protocols, CCITT Recommendation X.25 provides only the DTE/DCE interface specifications for operating in the packet mode on public data networks.

The recommendation, as currently structured, is not an end-to-end protocol although it does have end-to-end effects. Some controversy exists over whether or not the transport mechanism (such as X.25) should be structured as an end-to-end protocol. There is general agreement that higher level user-to-user or end-to-end protocols are required in addition to other standards and conventions to enable meaningful information interchange and the sharing of resources in a heterogeneous computer network environment.

End-to-end transport protocols would not be necessary where there is great confidence in lower level checking capabilities (no lost, duplicated, garbled or misrouted packet). Except for the most sensitive applications, e.g., funds transfer, the integrity of an X.25 network should be quite adequate. The virtual call service of X.25 could be viewed in the same light as a circuit switched connection between a user terminal and host computer. This transport mechanism has been designed to function transparently with respect to all higher levels of protocol. The only possible consideration that should enter into the design of higher level protocols is the economic consideration. The situation of frequently exceeding the maximum packet size should be avoided so that additional packets with very small quantities of user data do not need to be sent.

Summary of the advantages and disadvantages of the various end-to-end protocols that have been proposed or are in use.

Only two options are available with regard to interchange of character-oriented information between two or more data processing installations. Options are available to:

(1) Use identical computer architectures at each location and interchange character-oriented information in the native code and formats of those computers.

(2) Interchange character-oriented information using only strings of standard characters, such as ASCII. If necessary, convert to the various native codes and formats (such as compressed data, packed decimals, binary, floating point forms, etc.) to the standard strings.

Both techniques have been adopted in the industry. Certain corporations have converted to a single brand of computer to achieve the first option. In large organizations, this option often results in a recognized loss of "richness" in the varied capabilities available following the conversion to a single brand of computer.

A well-known example of the second option is the ARPA computer network which links various types of computers internationally. A network protocol is, of course, essential to its successful operation.

The international controversy regarding the need for an end-to-end transport protocol should not confuse the issues at higher levels of protocol. The design of application protocols can and should be accomplished independently of the transport protocol. The primary requirement on the transport protocol is reliable data transfer and this can be achieved in a number of different ways. Application protocols, on the other hand, are inherently end-to-end.

Although many networks of computers are now in operation, there are presently no standard end-to-end protocols. A proposed international end-to-end protocol is presented in document ISO/TC97/SC6-N1282 (CNP-49). This document was submitted to SC6 by the International Federation for Information Processing (IFIP) Working Group 6.1 (Packet Switched Network Interworking) in 1976 May. However, this is a proposal for a transport protocol. Only recently have groups in ISO and IFIP begun to consider end-to-end application protocols. Participation in such developments is active and much controversy is in evidence in the working papers generated in the USA and elsewhere on this topic.

It appears certain that packet switching will be employed to support widespread networks, and that many private end-to-end protocols will be built on top of common transport protocols such as X.25.

REFERENCES

Carr, C.S.; Cocker, S.D.; Cerf, V.G. Host-host communication protocol in the ARPA network: Proceedings of the Spring Joint Computer Conference; 1970 May: 589-597.

Cotton, Ira W. Computer network interconnection: problems and prospects; NBS Special Publication 500-6. 1977 April: 83 pages.

ISO/TC97/SC6 Document No. 1282. Proposal for an International End-to-End Protocol. 1976 May. 30 pages.

Meltzer, H.S.; Ickes, H.F. Information interchange between dissimilar systems. Modern Data. 56-57. 1971 April.

APPENDIX C: GLOSSARY

The following terms have been defined within the context in which they were used by the Task Force in this report. The Task Force recognizes that this glossary does not contain full and complete definitions of terms; rather, its purpose is to facilitate understanding of the proposed protocol.

Whenever possible, terms and definitions currently accepted as standards were used. However, certain inconsistencies with previous terminology may occur since the report has introduced several new concepts for which terms had to be assigned. The library networking community currently is preparing a consistent vocabulary of terms. This glossary has been prepared in coordination with that effort.

Account Number (Field)*

A unique code number that permits identification of transactions of a particular user, process, or message; used for billing, accounting and access purposes. Account numbers will be recorded by the Registry.

Accounting Method (Field)

The algorithm which the target host uses to figure the cost of services for a session. Accounting methods will be registered and assigned a unique identifying number in the Registry.

Acknowledgement (Message)

A message sent by a host to indicate that the previous message was received and that the Address/Reference Field was valid.

Acknowledgement Required Indicator

A bit, in the Flags portion of the Address/Reference Field, which indicates if the source host requires an Acknowledgement Message be sent by the destination host.

Address/Reference (Field)

A set of subfields used to route messages at the application level and to coordinate message exchange at each host. See also: Flag(s), Host ID, Reference Number, Session Number.

---

* The expression (Field) indicates that a field has been defined in this protocol and that the term preceding "(Field)" names the field.

Application Level Protocol

A standardized communications procedure that an application program (or more precisely the range of application programs that may exist in a library and information service environment) at one host computer uses to address another application program operating on a different host computer.

Application Process

A collection of computer programs, operating on a host computer, which perform a specific function such as On-line Cataloging, Acquisitions, Reference, etc.

Begin Session (Message)

The first message of a session sent by the originating host to the target host to establish a session, and to select the process at the target host. The target host sends a Begin Session Response Message to the originating host to indicate the establishment of a session.

Bibliographic Component

That portion of the National Library and Information Services Network that encompasses its bibliographic systems and segments of its communications system as opposed to library resource sharing or the total information community.

Communications Subnetwork

The physical telecommunications network interconnecting host computers.

Communications Protocol

See Protocol.

Connection

A circuit (either physical or virtual) connecting two host computers on the network.

Continue (Message)

A message sent by a host to indicate that the internal condition which previously caused it to send a Wait Message has been alleviated, and messages can again be received. See also: Wait (Message).

Continuation Indicator

A bit, in the Flags portion of the Address/Reference Field, which indicates that the source host has additional data messages associated with this transaction to send to the destination host.

Control Message

A message, sent between hosts on the network, which manages, supervises and coordinates the message flow at the application level.

Data Code (Field)

A registered number that specifies the coding convention used in the data portion of the message (e.g., ASCII or EBCDIC for character data, binary or packed decimal for numeric data).

Data Format Number (Field)

A registered number specifying the format of the data portion of the messsage (e.g., MARC Book Communication Format, Author-Title Key, Number of Hits).

Data Message

A message that contains the information pertinent to the proper execution of an application function executing at a target host on behalf of an originating host (e.g., Search, Catalog Input, Search Response).

Date and Time Stamp (Field)

The date and time in the ISO standard format.

Deadline

See: Time Deadline

Destination Host

The host on the network to which a message is sent by the source host.

End Session (Message)

The message sent by the originating host to the target host requesting that the session be ended. The target host terminates the session by sending an End Session Response Message to the originating host.

End-to-End Level Protocol

A transport protocol to allow reliable interprocess data transfer between host computers on a network.

Exception (Message)

A message sent by a host whenever it detects an unusual or exceptional condition as a result of, or as a by-product of, processing a message from another host.

Field

A specified area of a message used for a particular category of data or for specific data element. See also: Header Field.

Field Identifier (FID)

A unique number used to designate the Field Value subfield content. See also: Header Field.

Field Length (FL)

A number used to specify the length of the Field Value subfield content. See also: Header Field.

Field Value (FV)

The data in the Field Value subfield of the Header; identified by the Field Identifier. See also: Header Field.

Flag(s)

A portion of the Address/Reference Field, each bit of which has a specific meaning. See also: Source/ Destination Indicator, Acknowledgement Required Indicator, Continuation Indicator.

Forwarding

The process of a destination host passing a message on to another host which would respond directly to the source host.

Hardware Level Protocol

The protocol which controls the physical, electrical, functional and procedural characteristics to establish, maintain and disconnect the physical link between data communications equipment and data terminal equipment (e.g., RS-232,, Z.21).

Header

The first part of a message; contains information for directing that message to its destination and for controlling that message. The Header comprises discrete Header Fields. See also: Header Field.

Header Field

The discrete portion of a Header which contains information to control the message and session. A Header Field is comprised of three portions: Field Identifier, Field Length and Field Value. See also: Field Identifier, Field Length and Field Value.

Higher Level Protocol

A protocol or layer which is more removed from the electrical or link levels of a connection than another level; e.g., the Application Level Protocol is a higher level protocol than the Network Level Protocol.

Host

An institution and its associated computing equipment which is attached to a network and which provides library, bibliographic and information services.

Host Computer

A computer, attached to the network, that provides library, bibliographic and information services. See also: Host.

Host Identifier (ID)

A numeric code assigned in the Registry for a specific host and used for routing in the Address/Reference Field. See also: Address/Reference Field.

Last Reference (Field)

A field which contains two subfields and which shows the reference numbers of the last Data Messages sent by the originating host and target host. See also: Reference Number.

Layered Protocols

An approach to protocol design which isolates individual groups of functions and allows them each to be implemented independently (in a separate layer or level) from the other groups of functions.

Link Level Protocol

The control or processing procedures for the exchange of data between two directly connected points of a communications subnetwork.

Lower Level Protocols

A protocol level or layer which is less removed from the electrical or link levels of a connection than another level. See also: Higher Level Protocols.

Message

The unit of information transmitted between applications on the Network.

Message Resource Limit (Field)

See Resource Limit (Field).

Message Type (Field)

Representations of message type numbers which designate the message type. Message type numbers are assigned in the Registry, each uniquely identifying the type of message being sent, e.g., Begin Session Message, Acknowledgement Message, Pre-Cataloging Search Message, Search Response Message.

National Library and Information Service Network

A system consisting of host institutions and their associated functions, services and computing equipment; a telecommunications network; and resource sharing system; to facilitate access to the nation's library and information resources.

Network

See: National Library and Information Service Network.

Network Interface Processor

Computing equipment which performs the function of converting from internal host computer format to Network format.

Network Level Protocol

The control and processing procedures for the exchange of data across a data communications subnetwork.

Network Switching Processor

Computing equipment in a network which performs the functions of routing data to adjacent equipment across a telecommunications link.

Octet

A group of eight binary digits. Sometimes referred to as an eight-bit byte.

Originating Host

The host computer which initiates a session by sending a Begin Session Message to the target host and which requests services of the target host.

Originating Host Identifier (ID)

See Host Identifier (ID).

Password (Field)

A data element, required by a target host, and recognizable by automatic means, that permits an originating host to establish a session, perform select operations, access secure data, etc., on a target host.

Priority (Field)

A number assigned to a session specifying its relative processing sequence among other processes and sessions.

Process

See: Application Process.

Process Identifiers (ID) (Field)

A number, assigned in the Registry, which identifies the process invoked at a target host by an originating host.

Protocol

A formal set of conventions governing the format and relative sequencing of message exchange.

Purge (Message)

A request by one host to another host to immediately terminate the processing of either a message or a session.

Real Communications Path

The physical path which data follow when they are transmitted between two entities within the network.

Reference Number

A control number assigned and controlled by the originating host (Originating Host Reference Number) or by the target host (Target Host Reference Number) and shown in the Address/Reference Field of each message to provide continuity of messages and transactions.

Registry

A facility which functions as a depository for the current, up-to-date and correct version of the protocol and as an assigner of control codes for inclusion in the Field Identifiers and Field Values of Header Fields.

Resource Limit (Field)

A number that represents the amount of money an originating host is willing to spend at a target host in the processing of a session or message.

Resources Used (Field)

A number that represents the amount of money an originating host has spent at a target host during the processing of a session or message.

Response Data Code (Field)

A number that represents the coding convention used in the data portion of the Response Message which a source host requests that a destination host send. See also: Data Code.

Response Format Code (Field)

A code that represents the format of the data portion of the Response Message which a source host requests that a destination host send. See also: Data Format.

Response Type (Field)

A number that represents the message type of a Resource Message which a source host requests that a destination host send. See also: Message Type.

Resume (Message)

A message sent to begin processing again after having received a Suspend Message. See also: Suspend Message.

Session

An association between a process at one host and a process at another host, beginning with an explicit establishment sequence (Begin Session/Begin Session Response), through a sequence of control and data messages exchanged between hosts, and ending with an explicit termination sequence (End Session/End Session Response, Purge Session, etc.).

Session Number

A number assigned by an originating host during session establishment and used for the duration of a session in the Address/Reference Field of each message.

Session Resource Limit (Field)

See: Resource Limit (field).

Source Host

The host sending a message to destination host.

Source/Destination Indicator

A bit in the Flags portion of the Address/Reference Field which indicates whether the originating host is the source or destination of a message.

Status Code (Field)

A registered number that represents the current processing state of a session or message at the source host.

Status Query (Message)

A message sent to request the current status of another host regarding a current session. A Status Query Response (Message) is returned indicating the host's current processing state.

Suspend (Message)

A message sent by a source host to inform the destination host that it has temporarily ceased processing a message pending further information from the destination host. The destination host causes the source host to continue processing by sending a Resume Message (with appropriate data).

Target Host

The host which provides services to the originating host and, therefore, the host to which the originating host sends a Begin Session Message.

Target Host ID

See: Host ID.

Time Deadline (Field)

The date and time in ISO standard format when processing of a message is to be completed.

Transaction

A logical grouping of messages in both directions between originating and target hosts on a network.

Virtual Communications Path

A connection between entities on a network that may be realized by different physical configuration during transmission of messages. See also: Real Communications Path.

Wait (Message)

A message sent by a host when it wants to signal the other host to temporarily stop sending messages. A Wait is terminated by sending a Continue Message. See also: Continue (Message).

APPENDIX D: SUMMARY OF HEADER FIELDS PRESENT IN MESSAGES

MESSAGE TYPES / HEADER FIELDS		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
FV	Name	Address/ Reference	Message Type	Account No.	Password	Process ID	Session Resource Limit	Message Resource Limit	Status	Last Reference	Session Resources Used	Message Resources Used	Accounting Method Choice	Date & Time Stamp	Data Format	Data Code	Response Type	Response Type	Response Data Code	Priority	Time Deadline
1	Begin Session	R	R	R	O	R	O						O	O	I	I	I	I	I	O	
2	Begin Session Response	R	R			O			R					O	I	I	I	I	I		
3	End Session	R	R			O								O	I	I	I	I	I		
4	End Session Response	R	R						R		O			O	I	I	I	I	I		
5	Status Query	R	R											O	I	I	I	I	I		
6	Status Query Response	R	R	R		R			R	R	O	O		O	I	I	I	I	I	O	O
7	Purge Message	R	R											O	I	I	I	I	I		
8	Purge Message Response	R	R						R			O		O	I	I	I	I	I		
9	Purge Session	R	R						O		O			O	I	I	I	I	I		
10	Acknowledgement	R	R											O	I	I	I	I	I		
11	Exception	R	R						R					O	I	I	I	I	I		
12	Suspend	R	R						R					O	I	I	I	I	I		
13	Resume	R	R											O	I	I	I	I	I		
14	Wait	R	R											O	I	I	I	I	I		
15	Continue	R	R											O	I	I	I	I	I		

Legend: R = Required O = Optional I = Illegal Blank = Not Applicable

APPENDIX E: SAMPLE SESSION ILLUSTRATING HEADER FIELDS IN DETAIL

This appendix illustrates a hypothetical session consisting of a bibliographic search followed by an interlibrary loan transaction. The example was chosen to show the header fields in some detail. Because of its hypothetical nature, the data fields are left to the reader's imagination.

The session involves a total of 17 messages. Messages 1 through 3 establish the session. Messages 4 through 9 accomplish the bibliographic search. Messages 10 through 15 perform the interlibrary loan transaction. Messages 16 and 17 terminate the session.

Although many codes have already been specified in the protocol, for the sake of this example some additional code assignments have been arbitrarily made. In actual practice, such codes would be assigned to the registrar to have consistent meaning over the entire network.

In the graphic illustration of the sample session contained in this appendix, the contents of each octet is expressed as a decimal number, except in the header field values of the password and account number header, which are expressed in ASCII.

Header Length and Data Length are each two octets in length and are enclosed in a rectangular box. Throughout the header, the end of each header field is symbolized by a small filled-in triangle. Each octet or double-octet element is delimited by a small vertical mark.

When data fields are present in the messages they are not shown in detail but rather are symbolized by the letter 'n' in Data Length and a wavy line to indicate that the data portion of the message itself follows.

Header Field Values Used in the Sample Session

Field 1, Address/Reference
Flag values as defined by the Protocol
0 Message flow is from Originating Host to Target Host
1 Message flow is from Target Host to Originating Host
3 Message flow is from Target Host to originating Host, acknowledgement required
Other field values, arbitrarily assigned
5 Originating Host Identifier
57 Target Host Identifier
20 Session Number
Reference Number values are discussed further below.

Field 2, Message Type
Values defined by the Protocol as Control Message Types
1 Begin Session
2 Begin Session Response
3 End Session
4 End Session Response
5 Status Query
6 Status Response
10 Acknowledgement
Values arbitrarily chosen as Data Type Messages
40 Search
41 Search Response
42 Record Request
43 Record Response
44 Interlibrary Loan Availability Request
45 Interlibrary Loan Availability Response
46 Interlibrary Loan Transaction Request
47 Interlibrary Loan Transaction Response

Field 5, Process Identification
80 Interlibrary Loan

Field 8, Status
0 Process no longer active, terminated successfully
1 Process initiated successfully
3 Process actively processing a request

Fields 14 and 17, Data Format and Response Format
0 Plain Text
1 Formatted Author/Title Search Key
2 MARC Record
3 Record Number
4 Integer

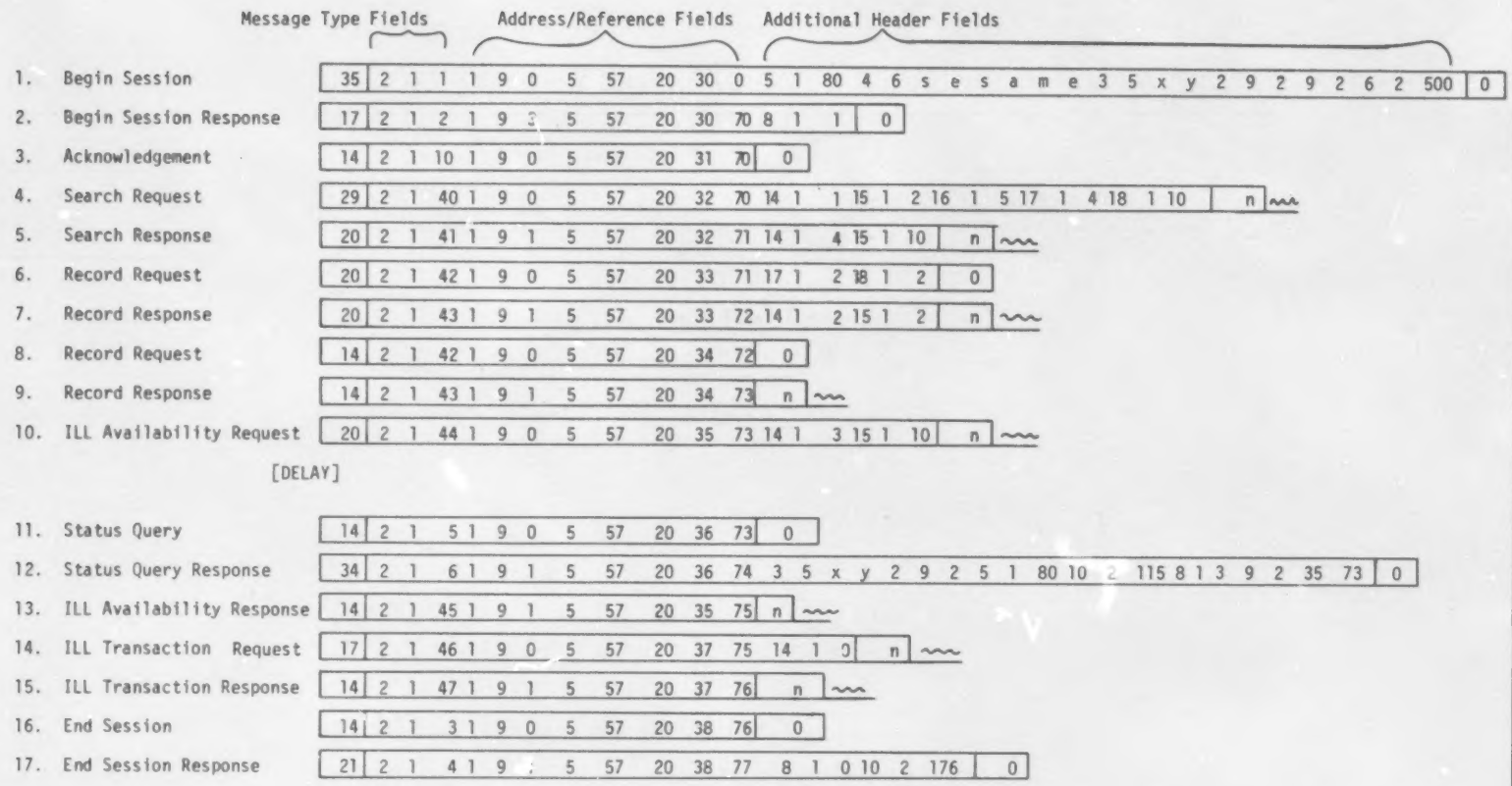
Fields 15 and 18, Data Code and Response Data Code
2 ASCII
10 Binary

Field 16, Response Type
5 Number of Hits

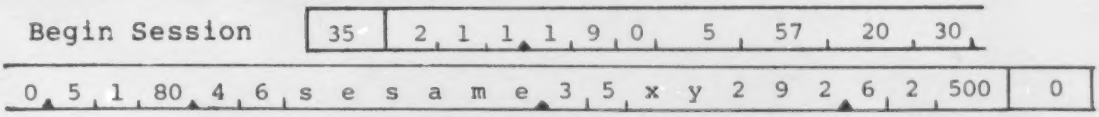
Further Discussion of the Address/Reference Field

Throughout the session, the Originating Host Identifier, the Target Host Identifier, and the Session Number remain constant. The values of the Flags element vary depending on the direction of message flow and whether or not an acknowledgement is requested. Even-numbered Flag values indicate that the message is flowing from the Originating Host to the Target Host. Odd-numbered Flag Values indicate that the message flow is in the reverse direction. Message number 2, in addition, has the acknowledge bit turned on, showing that an acknowledgement is expected from the Originating Host when this message is received.

In this sample session, the Originating Host assigns a value of 30 to its initial message number and the Target Host assigns a value of 70. For simplicity and ease of understanding in this example, the two hosts then assign sequentially higher numbers to each succeeding message. In fact, any algorithm for unambiguously assigning message numbers is acceptable since the numbering scheme used by the partner is assumed to be meaningless to the recipient. The reference number usage from message number 10 through message number 13 is particularly instructive. Message number 12 is numbered to show that it is a response to message 11 while message 13 is a response to message 10.

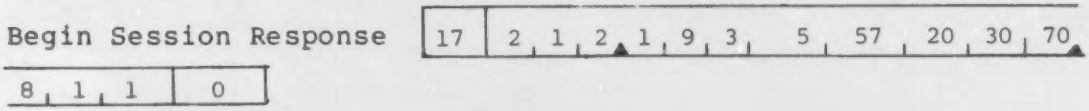
TABLE E.1: OVERVIEW OF THE SAMPLE SESSION

Detailed Discussion of Each Message in the Sample Session

1. Begin Session



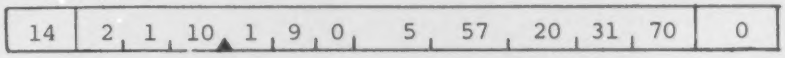
The Originating Host requests initiation of an Interlibrary Loan session. Password is "sesame," account number is "xy292" and session resource limit is $5.00.

2. Begin Session Response



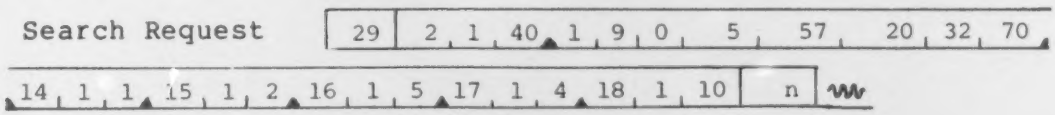
The Target Host responds by confirming successful initiation of the session in status header. Target Host requests acknowledgement of this message.

3. Acknowledgement



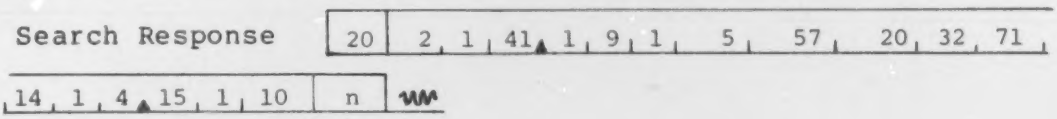
The Originating Host acknowledges Target Host's Begin Session Response.

4. Search Request



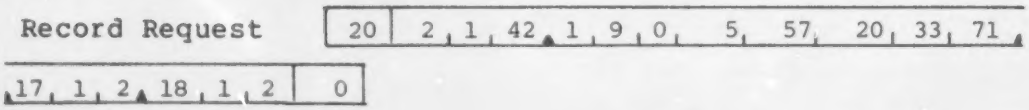
The Originating Host requests a bibliographic search of the data base at the Target Host. Originating Host supplies a formatted author/title search key in the Data portion of this message. The search key is encoded in ASCII. A response is to be supplied as a binary integer.

5. Search Response



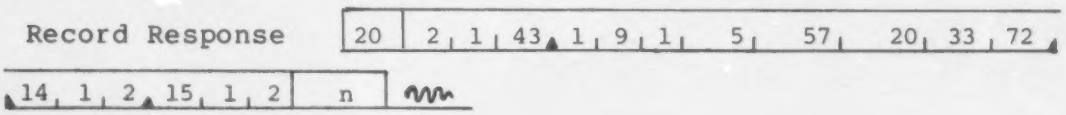
The Target Host replies by supplying the required number of hits as a binary integer in the data portion of the message.

6. Record Request



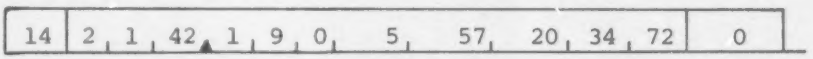
The Originating Host asks the Target Host to send the first record of the sequence of bibliographic records identified as a response to the search request in message number 4. The record is to be supplied in MARC format encoded in ASCII.

7. Record Response



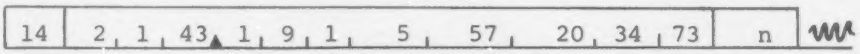
The Target Host responds by sending a record in MARC format, encoded in ASCII, in the data portion of the message.

8. Record Request



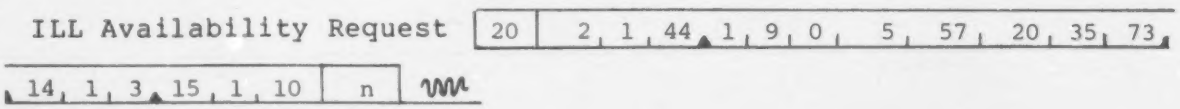
The Originating Host requests the next record in the sequence, implicitly asking that it be supplied in the same format and data code as specified in the preceding request.

9. Record Response



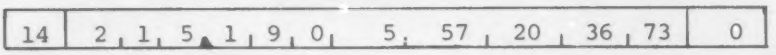
The Target Host responds by sending another record in MARC format, encoded in ASCII.

10. ILL Availability Request



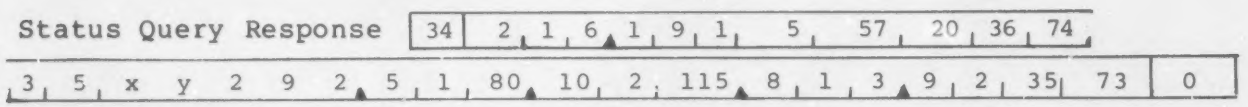
The Originating Host, presumably after inspecting the records supplied by the Target Host, requests information as to the availability, for Interlibrary Loan purposes, of the bibliographic item described by one of the records. Originating Host describes the desired item by supplying a record number in binary.

11. Status Query



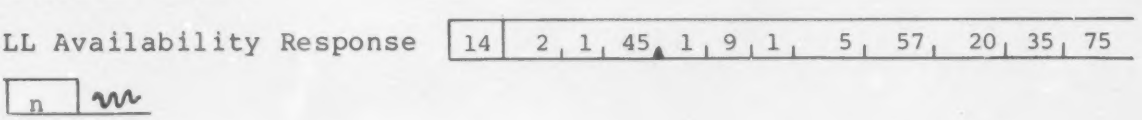
After perceiving an untimely delay in receiving a response to message 10, the Originating Host sends a Status Query.

12. Status Query Response



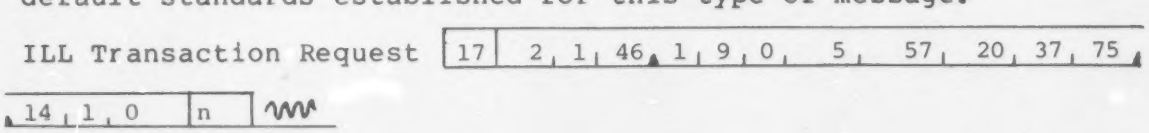
The Target Host responds by confirming the account number, indicating that the session involves an Inter-library Loan process, that $1.15 of the session resources has been used, that a message is being processed, and from its reference numbers it can be seen that the message being processed is the ILL Availability Request, message number 10 above.

13. ILL Availability Response



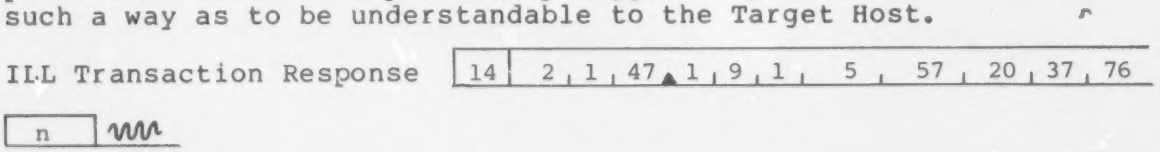
The Target Host gives a substantive response to the ILL Availability Request. Since no further header fields are included, the data portion can be assumed to conform to default standards established for this type of message.

14. ILL Transaction Request



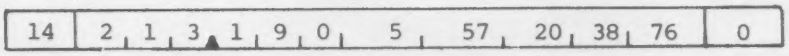
The Originating Host, after analyzing the Availability Response, now selects a library from which to request loan of the material. The transaction is supplied as a plain text data field presumably tagged or punctuated in such a way as to be understandable to the Target Host.

15. ILL Transaction Response



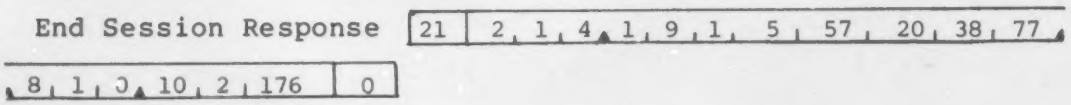
The Target Host responds by confirming the ILL Transaction Request together with whatever other pertinent data might be required for bookkeeping purposes to control the physical item involved. Again, the data portion conforms to default standards regarding format and code.

16. End Session



The Originating Host asks for termination of the session.

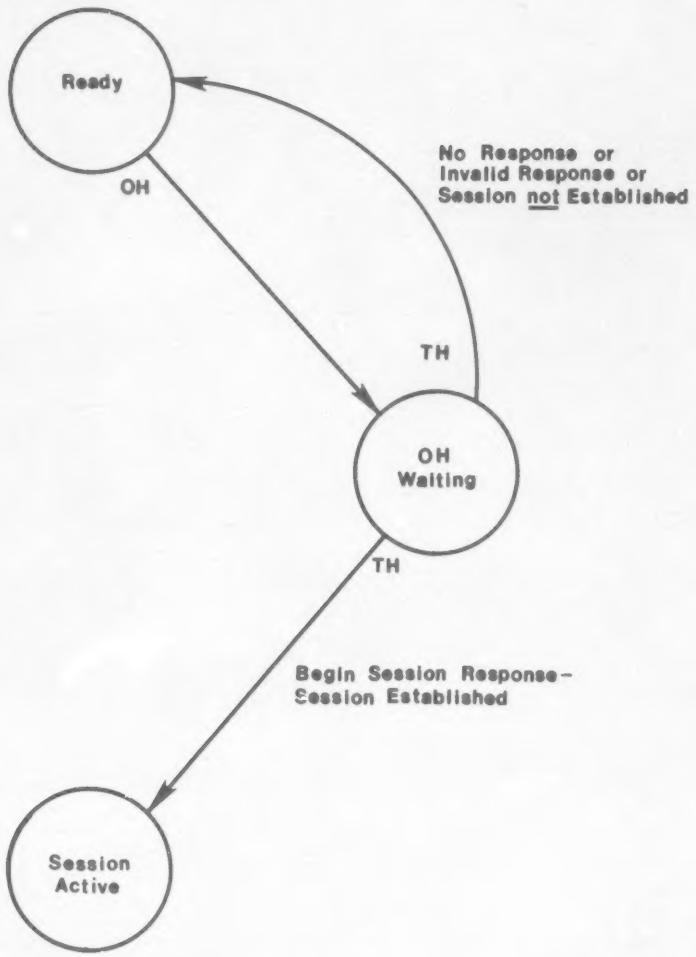
17. End Session Response



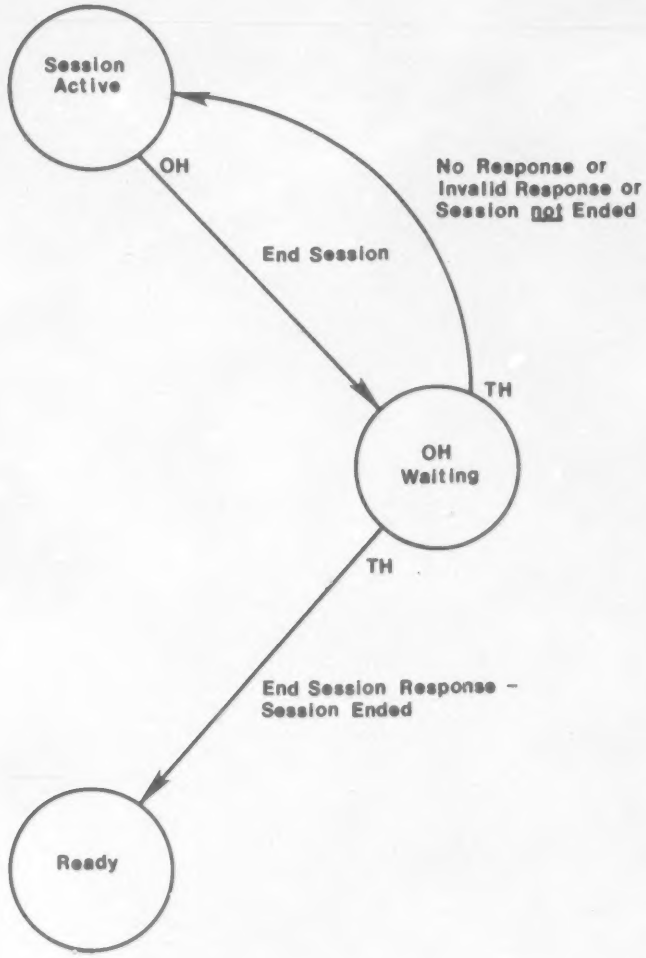
The Target Host responds that the session has been terminated normally and that the cost for processing on the Target Host is $1.76 for the entire session.

APPEN STATE DIAGRAMS

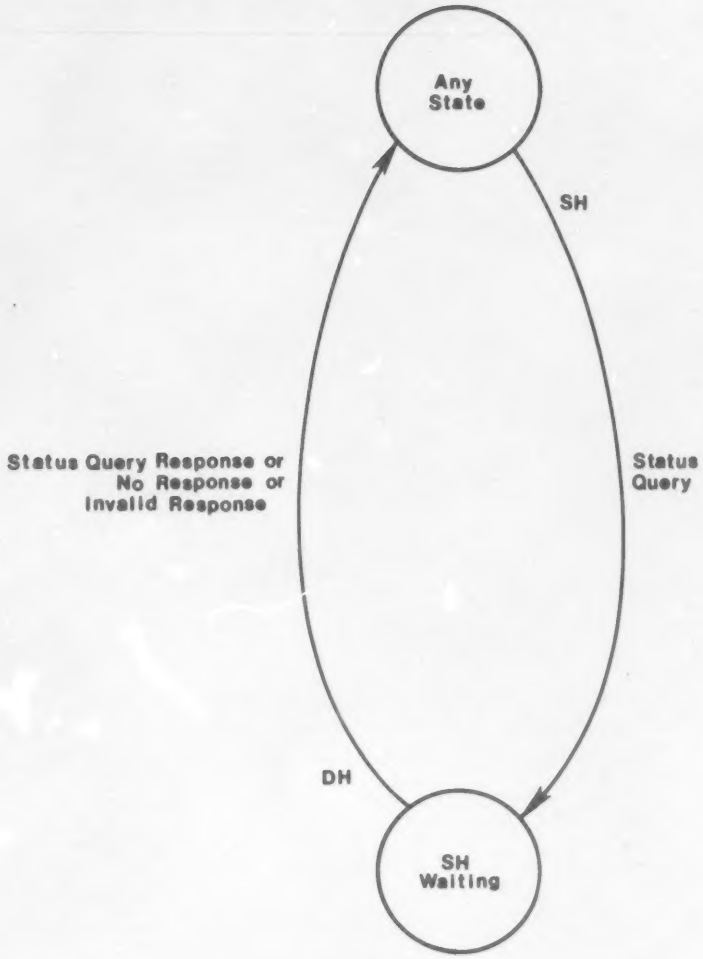
The following state diagrams illustrate the session flow for various messages. In these diagrams, OH = originating host, DH = destination host, SH = source host and TH = target host.



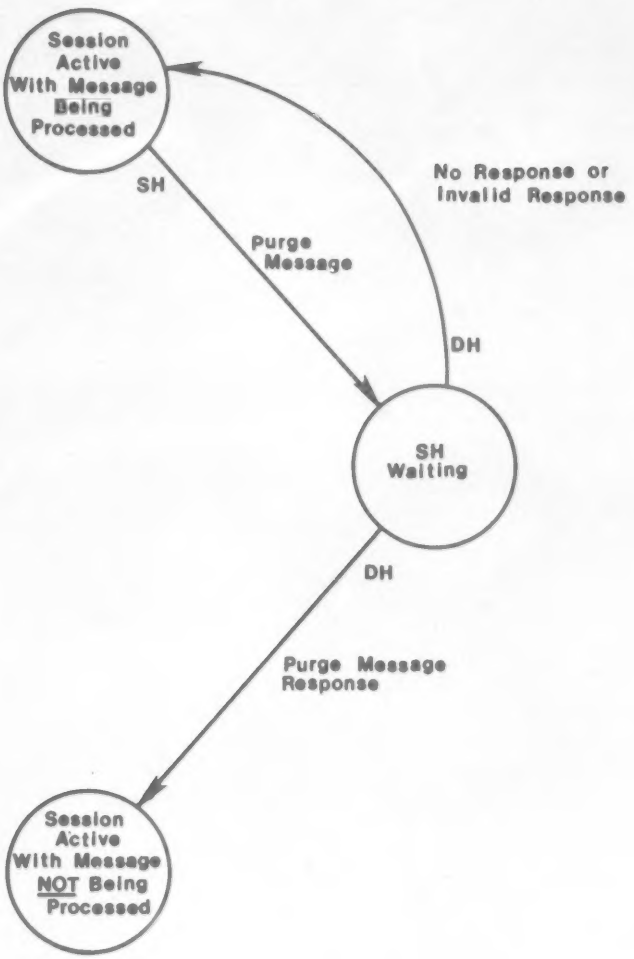
BEGIN SESSION PHASE



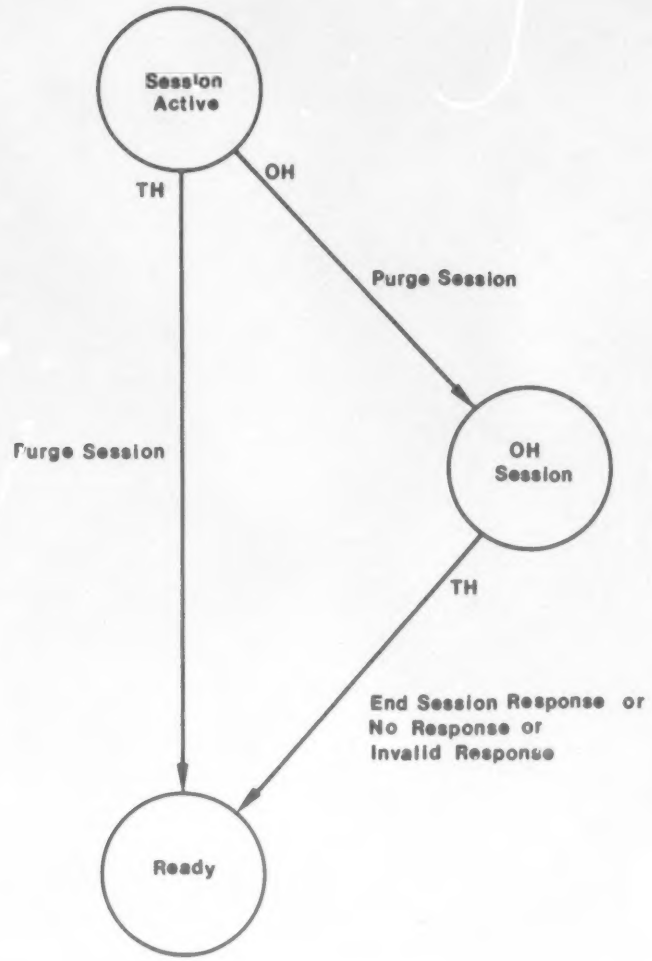
END SESSION PHASE



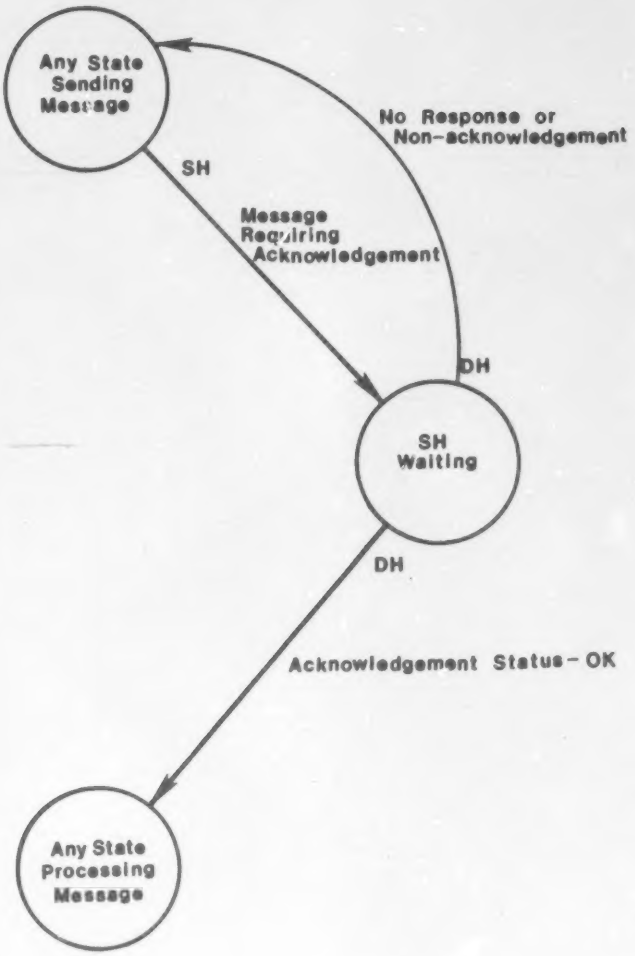
STATUS QUERY/RESPONSE PHASE



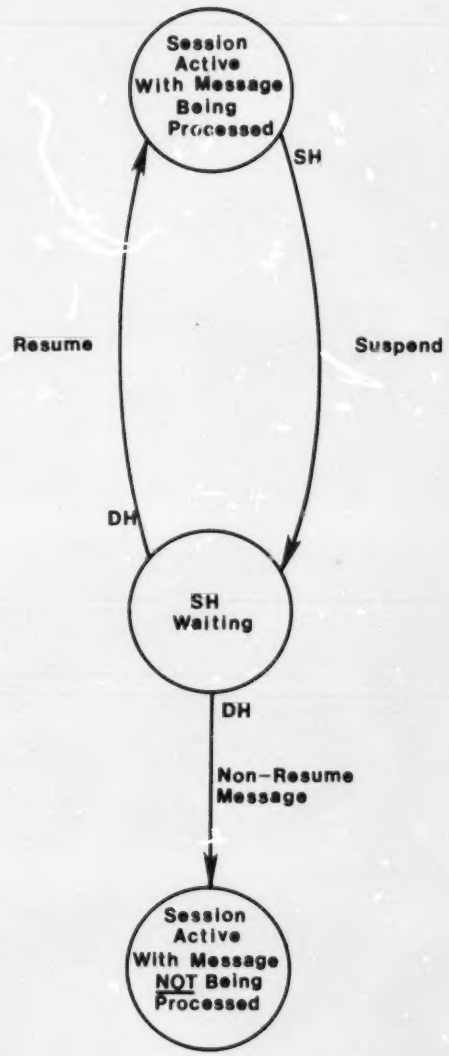
PURGE MESSAGE PHASE



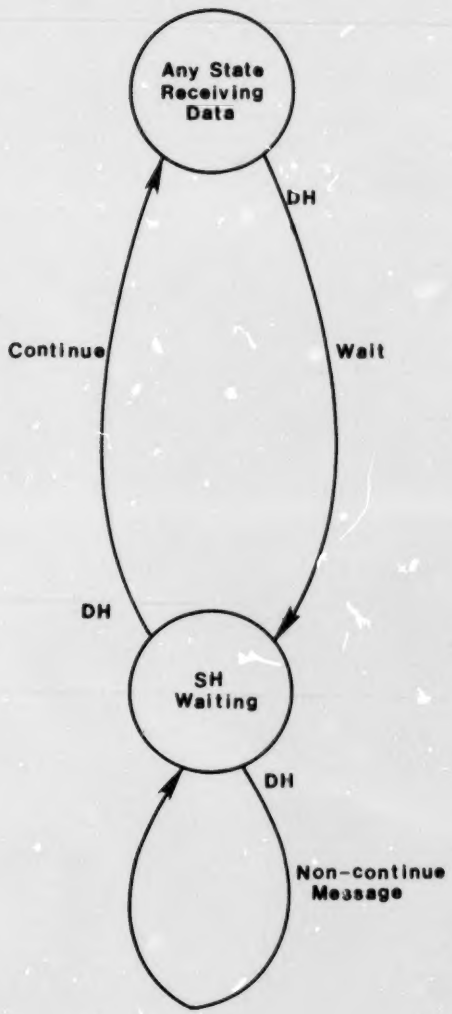
PURGE SESSION PHASE



ACKNOWLEDGEMENT PHASE



SUSPEND/RESUME PHASE



WAIT/CONTINUE PHASE

APPENDIX G: BIBLIOGRAPHY

I. NETWORK AND NETWORK PROTOCOLS

Carr, C. S.; Crocker, S. D.; Cerf, V. G. Host-host communications protocol in the ARPA network. Proceedings of the Spring Joint Computer Conference; 1970. 589-597.

Computer Communications Group. Standard network access protocol (SNAP) specifications. Ottawa, Canada: Trans-Canada Telephone System; 1976 March 31. 83p.

Cotton, Ira W. Computer network interconnection: problems and prospects. NBS Special Publication 500-6; 1977 April. 83p.

Cotton, Ira W. Net results, layering of protocols. Computer Decisions. 8(8): 14; 1976 August.

Day, John. Aspects of good protocol definition. Subcommittee on the Formal Definition of Protocols; 1976 September 20; IFIF WG 6.1. 3 p.

Feinler, Elizabeth; Postel, Jon. ARPANET protocol handbook. Menlo Park, California: Network Information Center, Stanford Research Institute; 1976 April; NIC 7104, Revision 1.

Kimbleton, S. R.; Schneider, G. M. Computer communication networks: approaches, objectives and performance considerations. Computing Surveys. 7(3): 129-173; 1975 September.

Proposal for an international end-to-end protocol. International Federation of Information Processing (IFIP); 1976 May. ISO-TC97/SC6 N1282.

Rosenthal, Robert. A review of network access techniques with a case study: the network access machine. 1976 July; NBS Technical Note 917. 36p.

Schicker, P.; Duenki, A.; Baechi, W. Bulk transfer function (proposal). European Informatics Network; 1975 September; INWG Protocol 31, EIN/ZHR/75/20. 24p.

Schicker, P.; Duenki, A. Virtual terminal definition and protocol. European Informatics Network Document EIN/ZHR/76/019; 1976 July. 28p.

Van Velze, P. EURONET--present state of development. Luxembourg: Network Technical Operations, CEC, EURONET Host Information Meeting; 1977 January 10-11; EHG/8/77. 18p.

Wood, H. M.; Watkins, S. W.; Cotton, I. W. Annotated bibliography of the literature on resource sharing computer networks. NBS Special Publication 384; 1976 September. 179p.

II. LIBRARY NETWORK PLANS

Avram, Henriette D.; Maruyama, Lenore S. (eds). The library bibliographic component of the national library and information service network. Washington, D.C. Library of Congress Network Advisory Group; 1977 March; Preliminary Edition. 91p.

Technical communications, protocol for computer-to-computer communication. Journal of Library Automation. 9(2): 167-191; 1976 June.

Toward a national program for library and information services; goals for action. Washington, D.C.: National Commission on Libraries and Information Science; 1975. 119p.

III. COMMUNICATIONS AND INTERFACE STANDARDS

American national standard code for information interchange (ASCII). Washington, D.C.: American National Standards Institute; 1977 June 9. ANSI X3.4-1968. 15p.

Document from international organization for standardization (ISO) technical committee 97 on computers and information process (TC 97) subcommittee 6 on data communications (SC6) on high level data link control (HDLC) heading formats. 1976 April. ANSI X3S33/76-22.

Editors Group on X.25. Completion of level 2 of recommendation X.25. Geneva: CCITT Study Group VII; 1977 April 19-26; Temporary document no. 60-E, Level 2. 30p.

Fifth draft, proposed American national standard for advanced data communication control procedures (ADCCP). 1976 April 9. ANSI X3S34/589.

Folts, Harold C.; Cotton, Ira W. Interfaces: new standards catch up with technology. Data Communications. 31-40; 1977 June.

HDLC heading formats. U.S. contribution. Submitted to W. F. Emmons, Rapporteur. 1976 October; ISO/TC97/SC6 Document No, 1308. ISO Project 24. 4p.

Interface between data terminal equipment and data circuit-termination equipment for terminals operating in the packet mode on public data networks. Washington, D.C.: International Consultative Committee on Telegraph and Telephone (CCITT). Recommendation X.25, ANSI document X3S37/76-14, updated 1976 document.

Message heading formats for information interchange using the ASCII for data communication system control. Washington, D.C.: Draft Proposed American National Standard; 1974 November. ANSI BSR X3.57, X3S33/125. 17p. plus 6 appendixes and expository remarks.

Procedures for the use of the communication control characters of ASCII in specified data communication links. Washington, D.C.: proposed Revised American National Standard; 1973 January. ANSI BSR X3. 28, X3S34/437. 185p.

Ross, H. McGregor. Report on standards on computing, Part C--communications. London: Data Systems Consultants; 1976 July. 54p.

Standardization of information field format and function for communication purposes. Rapporteur Report on Project 24; 1976 October. ISO/TC97/SC6 Document No. 1309. 19p.

IV. DATA REPRESENTATION STANDARDS

ANSI standard X3.51-1975. Representations of universal time, local time differentials, and United States time zone references for information interchange. 1975 August 3.

ISO 3307-1975. International standard. Information interchange, representations of time of the day. 1975 March 15. first edition 2p.

V. DEFINITIONS, GLOSSARY, TERMINOLOGY

Duncan, B. C.; Garvin, D. Complete clear text representation of scientific documents in machine-readable form. 1974 February NBS TN 820. 55p.

Meltzer, H. S.; Ickes, H. F. Information interchange between dissimilar systems. Modern Data. 4(4): 56-67; 1971 April.

Neumann, Albrecht, J. Proposed implementation for development of user-terminal protocols for computer network access. NBS IR 75-744; 1975 July. 17p.

☆ U.S. GOVERNMENT PRINTING OFFICE : 1978 O—274-286